# 湖南省中西医结合医院
# （湖南省中医药研究院附属医院）

# 网络安全等级保护测评及安全服务采购

# 招标文件

## 招标编号：ZTBB202339

## 2023 年 10 月

# 目录

# 第一部分 招标书

我院因业务发展需要，拟购置**网络安全等级保护测评及安全服务项目**，现对该项目组织招标，诚邀各公司前来参与竞标。

1.招标编号：ZTBB202339

2.采购内容：**网络安全等级保护测评及安全服务**

3.招标内容：网络安全等级保护测评及安全服务（HIS 系统三级评测；LIS 系统三级评测；PACS 系统三级评测；EMR 系统三级评测；互联网医院系统三级评测；安全服务）；

4.投标商资格：

（1）投标商应具备《政府采购法》第二十二条规定的条件；

（2）在中华人民共和国境内注册的能独立承担民事责任的法人，依法取得营业执照，具有从事本项目的经营范围和能力；

（3）投标商必须具备所投项目的经营资格；

（4）投标人在参加政府采购活动前三年内，在经营活动中没有重大违法记录，在投标截止时间前未被列入失信被执行人、重大税收违法案件当事人名单，未被列入政府采购严重违法失信行为记录名单；

（5）有依法缴纳税收和社会保障资金的良好记录

（6）本项目不允许联合体投标；

（7）法律、法规规定的其他条件；

5.开标时间：另行通知；

6.开标地点：湖南省中西医结合医院（湖南省中医药研究院附属医院）综合办公楼四楼 411 会议室。

# 第二部分 投标方须知

## 一、投标要求

### 1、 合格的投标人和合格的服务

投标人必须具有独立法人资格或者具有独立承担民事责任的能力，遵守国家法律、行政法规，具有良好的信誉及履行合同的能力和良好的履行合同记录，资金状况良好的，有依法缴纳税收和社会保障资金的良好记录，参加采购活动前三年内，在经营活动中没有重大违法记录，具有与投标项目相应经营资质的公司，均为合格的投标人。凡经中华人民共和国政府有关部门批准注册，并具备相关质量管理体系认证，符合本次采购技术要求的服务，均为合格的服务。

### 2、 资质文件要求：

①投标单位营业执照

②投标单位法人身份证复印件（如投标人不是投标单位的法定代表人，须提供法人身份证复印件及法人代表授权书、授权人身份证复印件）

③具备公安部第三研究所颁发的《网络安全等级测评与检测评估机构服务认证证书》，附证书复印件及网站查询截图；

④具有中国网络安全审核技术与认证中心颁发的信息安全服务资质认证证书-信息安全风险评估资质、信息系统安全运维资质(提供相关证书复印件并盖公章)；

⑤具有 cncert 网络安全应急服务支撑单位省级及以上证书，附证书复印件（因第十届支撑单位名单未公布，以第九届为准）；

⑥近三年来（2020 年 9 月至 2023 年 9 月）未受到国家网络安全等级保护工作协调小组办公室警告、处罚、整改等处罚，相关信息在投标截止时间前在中国网络安全等级保护网（www.djbh.net）上进行查询佐证，附查询截图；

请提供上述文件复印件并加盖原厂公章，以上均为投标单位的必备文件，若投标单位未提供或不符合要求，经评委会同意可按无效投标处理。

### 3、 投标文件的编制和递交：

（1）投标格式（采用 A4 纸装订成册，页码由投标单位**自行编列**）：

①开标一览表；

②投标单位概况；

③招标文件要求提交的资质文件要求；

④项目偏离表；

⑤投标文件响应及报价清单；

⑥售后及相关承诺；

⑦上年度审计报告；

⑧近三个月纳税证明（开标前半年内任意连续三个月）；

⑨近三年类似案例证明；

⑩投标单位认为有必要提供的其他相关材料。

（2）投标货币：人民币。

（3）投标书的递交：投标人应准备投标文件正本 1 份，副本 1 份，并各自装订成册，密封于信封内，封口处加盖公章或由投标人签字。价格表正本一份，用信封**单独密封**一同报送，封口处加盖公章或由投标人签字。开标时每家投标单位可对项目进行一定时间现场讲解。。

（4）投标文件应于开标当天准时送达湖南省中西医结合医院（湖南省中医药研究院附属医院）开标现场。

**4、 投标报价：**

（1）项目限价 42.5 万元人民币以下；

（2）采取二次报价的办法。投标人报价表的价格视为第一次报价，经评委会补充有关要求后，评审前，投标人还可进行现场第二次报价(自备二次报价单)；

（3）招标后所确定的供货内容和成交价格，在合同执行过程中，不得以任何理由变更；

（4）本次招标在满足招标文件要求的基础上低价中标。

**5、 招标文件的澄清、修改：**

（1）在招标的任何时候，无论出于何种原因，湖南省中西医结合医院（湖南省中医药研究院附属医院）有权对招标文件进行修改。修改内容将以书面形式通知所有参与投标人，并作为原文件的补充，与其具有同等法律效力。

（2）招标文件的解释权归湖南省中西医结合医院（湖南省中医药研究院附属医院）。

**6、 纪律与保密**

（1）参与评审的人员应严守有关保密的法律、法规和规定，严格自律，并接受上级主管部门和有关主管部门的审计和监督。

（2）投标人申报的关于资质、业绩等文件和材料必须真实准确，不得弄虚作假。

（3）投标人不得串通作弊，哄抬标价，致使定标困难或无法定标。

（4）投标人不得采用不正当手段妨碍、排挤其他投标人，扰乱招标市场，破坏公平竞争。

（5）投标人不得以任何形式打听和搜集评标机密、干扰评审和授标工作。

（6）投标人若违反上述要求，其投标将被废除。

**二、评委会职能：**

（1）根据招标文件的要求，决定进入投标单位的名单；

（2）根据招标文件的要求，决定招标具体内容；

（3）有权对采购内容、技术要求和招标办法进行解释，有权决定处理招标过程中出现的其它相关问题。

**三、招标程序：**

招标的全过程为院方大致讲解内容要求、二次报价（最终报价）、阅读审查投标文件、评委评审几个阶段进行。

（1）投标报价：将各投标单位的投标文件中项目名称、单价、数量、总价、交货期、保质期、售后等内容均详细记录在册。

（2）评审：开标后，评委会通过阅读投标文件，进行具体的技术性、商务性评审。

A.符合性审查：对投标单位的资质，投标文件的内容进行商务和技术符合性的审查。投标文件中的数据大、小写不符，以大写为准；单价与总价不符，以单价为准。

B.技术评审内容：项目的技术指标、主要配置及伴随服务等。

C.商务评审内容：报价数据计算的正确性、完整性，分析报价构成的合理性，交货期，付款方式等。

**四、定标：**

定标程序：根据评委会的评审结果，由评委会定确定中标候选单位。由湖南省中西医结合医院（湖南省中医药研究院附属医院）对中标候选单位进行不少于三天的网上公示前三名排序。

**五、买卖合同：**

湖南省中西医结合医院（湖南省中医药研究院附属医院）与中标公司洽谈合同条款，签订买卖合同。招投标文件是签订买卖合同的依据。

# 第三部分 采购内容及技术要求

**一、采购内容：**网络安全等级保护测评及安全服务（HIS 系统三级评测；LIS 系统三级评测；PACS 系统三级评测；EMR 系统三级评测；互联网医院系统三级评测；安全服务）。

**二、技术要求：**

依据《信息安全技术网络安全等级保护基本要求》（GB/T 22239-2019）三级/二级要求，对信息系统进行等级测评，找出系统与国家标准要求之间的差距，对存在的风险进行评估，并出具《信息安全等级测评报告》和《安全建设整改方案》。测评内容涵盖：

1、安全物理环境

安全物理环境测评将通过访谈和检查的方式评测信息系统的物理安全保障情况。主要涉及对象为机房。在内容上，物理安全层面测评实施过程涉及 10 个安全子类，具体如下表：

| 序号 | 安全子类 | 测评指标描述 |
|---|---|---|
| 1 | 物理位置的选择 | 通过访谈物理安全负责人，检查机房，测评机房物理场所在位置上是否具有防震、防风和防雨等多方面的安全防范能力。 |
| 2 | 物理访问控制 | 通过访谈物理安全负责人，检查机房出入口等过程，测评信息系统在物理访问控制方面的安全防范能力。 |
| 3 | 防盗窃和防破坏 | 通过访谈物理安全负责人，检查机房内的主要设备、介质和防盗报警设施等过程，测评信息系统是否采取必要的措施预防设备、介质等丢失和被破坏。 |
| 4 | 防雷击 | 通过访谈物理安全负责人，检查机房设计/验收文档，测评信息系统是否采取相应的措施预防雷击。 |
| 5 | 防火 | 通过访谈物理安全负责人，检查机房防火方面的安全管理制度，检查机房防火设备等过程，测评信息系统是否采取必要的措施防止火灾的发生。 |
| 6 | 防水和防潮 | 通过访谈物理安全负责人，检查机房及其除潮设备等过程，测评信息系统是否采取必要措施来防止水灾和机房潮湿。 |
| 7 | 防静电 | 通过访谈物理安全负责人，检查机房等过程，测评信息系统是否采取必要措施防止静电的产生。 |
| 8 | 温湿度控制 | 通过访谈物理安全负责人，检查机房的温湿度自动调节系统，测评信息系统是否采取必要措施对机房内的温湿度进行控制。 |
| 9 | 电力供应 | 通过访谈物理安全负责人，检查机房供电线路、设备等过程，测评是否具备为信息系统提供一定电力供应的能力。 |
| 10 | 电磁防护 | 通过访谈物理安全负责人，检查主要设备等过程，测评信息系统是否具备一定的电磁防护能力。 |

2、安全通信网络

安全通信网络测评将通过访谈、检查和测试的方式评测信息系统的网络安全保障情况。主要涉及对象机房的网络设备、网络安全设备以及网络拓扑结构等三大类对象。在内容上，通信网络安全层面测评过程涉及个工作单元。

| 序号 | 安全子类 | 测评指标描述 |
|---|---|---|
| 1 | 网络架构 | 通过访谈网络管理员，检查网络拓扑情况、核查核心交换机、路由器，测评分析网络架构与网段划分、隔离等情况的合理性和有效性。 |
| 2 | 通信传输 | 通过访谈网络管理员，检查各硬件设备传输过程中是否采用加密技术。 |
| 3 | 可信验证 | 通过访谈网络管理员，检查各硬件设备传输过程中是否采用可信验证技术。 |

3、安全区域边界

安全区域边界测评将通过访谈、检查和测试的方式评测信息系统的边界防护，在内容上，安全区域边界测评实施过程涉及 6 个安全子类。

| 序号 | 安全子类 | 测评指标描述 |
|---|---|---|
| 1 | 边界防护 | 通过访谈网络管理员，查看边界设备防护措施。 |
| 2 | 访问控制 | 通过访谈网络管理员，查看边界设备的访问控制策略。 |
| 3 | 入侵防范 | 通过访谈网络管理员，查看各个关键网络节点的防入侵措施。 |
| 4 | 恶意代码防范和垃圾邮件防范 | 通过访谈网络管理员，查看各个关键网络节点恶意代码防范措施。 |
| 5 | 安全审计 | 通过访谈网络管理员，查看边界设备的日志审计策略和记录。 |
| 6 | 可信验证 | 通过访谈网络管理员，查看边界设备是否采用可信验证技术。 |

4、安全计算环境

安全计算环境测评将通过访谈、检查和测试的方式评测信息系统的应用安全保障情况。在内容上，安全计算环境测评实施过程涉及 11 个工作单元，具体如下表：

| 序号 | 安全子类 | 测评指标描述 |
|---|---|---|
| 1 | 身份鉴别 | 检查信息系统网络设备、安全设备、服务器、数据库和应用系统的身份标识与鉴别功能设置和使用配置情况；检查应用系统对用户登录各种情况的处理，如登录失败处理、登录连接超时等。 |
| 2 | 访问控制 | 检查网络设备、安全设备、服务器、数据库和应用系统的访问控制功能设置情况，如访问控制的策略、访问控制粒度、权限设置 |

| | | |
|---|---|---|
| | | 情况等。 |
| 3 | 安全审计 | 检查网络设备、安全设备、服务器、数据库和应用系统的安全审计配置情况，如覆盖范围、记录的项目和内容等；检查应用系统安全审计进程和记录的保护情况。 |
| 4 | 可信验证 | 检查计算设备的系统引导程序、系统程序、重要配置参数和应用系统程序等是否可以进行可信验证，并检测可信验证受到破坏时进行报警。 |
| 5 | 入侵防范 | 检查网络设备、安全设备、服务器、数据库和应用系统入侵防范，如关闭不需要的端口和服务、最小化安装、部署入侵防范产品等。 |
| 6 | 恶意代码防范 | 检查网络设备、安全设备、服务器、数据库和应用系统恶意代码防范措施。 |
| 7 | 数据完整性 | 检查网络设备、安全设备、服务器、数据库和应用系统的通信完整性保护情况。 |
| 8 | 数据保密性 | 检查网络设备、安全设备、服务器、数据库和应用系统的通信保密性保护情况。 |
| 9 | 数据备份和恢复 | 检查网络设备、安全设备、服务器、数据库和应用系统的关键信息备份情况。 |
| 10 | 剩余信息保护 | 检查网络设备、安全设备、服务器、数据库和应用系统。 |
| 11 | 个人信息保护 | 检查系统收集个人信息和使用个人信息的情况。 |

5、安全管理中心

在内容上，安全管理中心层面测评实施过程涉及 4 个工作单元，具体如下表：

| 序号 | 安全子类 | 测评指标描述 |
|---|---|---|
| 1 | 系统管理 | 通过访谈系统管理员，对系统的资源和运行配置进行配置、控制和管理是否全由系统管理员进行操作。 |
| 2 | 审计管理 | 通过访谈安全审计员，是否对审计记录进行分析，并根据分析结果进行处理，包括根据安全审计策略对审计记录进行存储、管理和查询等。 |
| 3 | 安全管理 | 通过访问安全员，对系统的安全策略进行配置，包括安全参数的设置、主体、客体进行统一安全标记，对主体进行授权，配置可信验证策略是否全由安全员进行操作。 |
| 4 | 集中管控 | 通过访谈安全员，对分布在网络中的安全设备或安全组件进行管控，对网络链路、安全设备、网络设备和服务器等的运行状况进行集中监测、对分散在各个设备上的审计数据进行收集汇总和集中分析，对安全策略、恶意代码、补丁升级等安全相关事项进行集中管理，对网络中发生的各类安全事件进行识别、报警和分析的情况。 |

6、安全管理制度

安全策略和管理制度测评将通过访谈和检查的形式评测安全管理制度的制定、发布、评审和修订等情况。主要涉及安全主管人员、安全管理人员、各类其它人员、各类管理制度、各类操作规程文件等对象。在内容上，安全管理制度测评实施过程涉及 4 个工作单元，具体如下表：

| 序号 | 安全子类 | 测评指标描述 |
|---|---|---|
| 1 | 安全策略 | 通过访谈安全主管，检查有关管理制度文档和重要操作规程等过程，测评信息系统管理制度在内容覆盖上是否全面、完善。 |
| 2 | 管理制度 | 通过访谈安全主管，检查有关制度制定要求文档等过程，测评信息系统管理制度的制定和发布过程是否遵循一定的流程。 |
| 3 | 制定和发布 | 通过访谈安全主管，检查管理制度评审记录等过程，测评信息系统管理制度定期评审和修订情况。 |
| 4 | 评审和修订 | 通过访谈安全主管，检查管理制度评审记录等过程，测评信息系统管理制度定期评审和修订情况。 |

7、安全管理机构

安全管理机构测评将通过访谈和检查的形式评测安全管理机构的组成情况和机构工作组织情况。主要涉及安全主管人员、安全管理人员、相关的文件资料和工作记录等对象。

| 序号 | 安全子类 | 测评指标描述 |
|---|---|---|
| 1 | 岗位设置 | 通过访谈安全主管，检查部门/岗位职责文件，测评信息系统安全主管部门设置情况以及各岗位设置和岗位职责情况。 |
| 2 | 人员配备 | 通过访谈安全主管，检查人员名单等文档，测评信息系统各个岗位人员配备情况。 |
| 3 | 授权和审批 | 通过访谈安全主管，检查相关文档，测评信息系统对关键活动的授权和审批情况。 |
| 4 | 沟通和合作 | 通过访谈安全主管，检查相关文档，测评信息系统内部部门间、与外部单位间的沟通与合作情况。 |
| 5 | 审核和检查 | 通过访谈安全主管，检查记录文档等过程，测评信息系统安全工作的审核和检查情况。 |

8、安全管理人员

安全管理人员测评将通过访谈和检查的形式评测机构人员安全控制方面的情况。主要涉及安全主管人员、人事管理人员、相关管理制度、相关工作记录等对象。

在内容上，人员安全管理测评实施过程涉及 4 个工作单元，具体如下表：

| 序号 | 安全子类 | 测评指标描述 |
|---|---|---|
| 1 | 人员录用 | 通过访谈人事负责人，检查人员录用文档等过程，测评信息 |

| | | |
|---|---|---|
| | | 系统录用人员时是否对人员提出要求以及是否对其进行各种审查和考核。 |
| 2 | 人员离岗 | 通过访谈人事负责人，检查人员离岗安全处理记录等过程，测评信息系统人员离岗时是否按照一定的手续办理。 |
| 3 | 安全意识教育和培训 | 通过访谈安全主管，检查培训计划和执行记录等文档，测评是否对人员进行安全方面的教育和培训。 |
| 4 | 外部人员访问管理 | 通过访谈安全主管，检查有关文档等过程，测评对第三方人员访问（物理、逻辑）系统是否采取必要控制措施。 |

9、安全建设管理

安全建设管理测评将通过访谈和检查的形式评测系统建设管理过程中的安全控制情况。主要涉及安全主管人员、系统建设负责人、各类管理制度、操作规程文件、执行过程记录等对象。

在内容上，系统建设管理测评实施过程涉及 10 个工作单元，具体如下表：

| 序号 | 安全子类 | 测评指标描述 |
|---|---|---|
| 1 | 定级和备案 | 通过访谈安全主管，检查系统定级相关文档等过程，测评是否按照一定要求确定系统的安全等级。 |
| 2 | 安全方案设计 | 通过访谈系统建设负责人，检查系统安全建设方案等文档，测评系统整体的安全规划设计是否按照一定流程进行。 |
| 3 | 产品采购和使用 | 通过访谈安全主管、系统建设负责人和安全产品等过程，测评是否按照一定的要求进行系统的产品采购。 |
| 4 | 自行软件开发 | 通过访谈系统建设负责人，检查相关软件开发文档等，测评自行开发的软件是否采取必要的措施保证开发过程的安全性。 |
| 5 | 外包软件开发 | 通过访谈系统建设负责人，检查相关文档，测评外包开发的软件是否采取必要的措施保证开发过程的安全性和日后的维护工作能够正常开展。 |
| 6 | 工程实施 | 通过访谈系统建设负责人，检查相关文档，测评系统建设的实施过程是否采取必要的措施使其在机构可控的范围内进行。 |
| 7 | 测试验收 | 通过访谈系统建设负责人，检查测试验收等相关文档，测评系统运行前是否对其进行测试验收工作。 |
| 8 | 系统交付 | 通过访谈系统运维负责人，检查系统交付清单等过程，测评是否采取必要的措施对系统交付过程进行有效控制。 |
| 9 | 等级测评 | 通过访谈系统运维负责人，核查定期开展等级测评和等级保护整改情况。 |
| 10 | 服务供应商选择 | 通过访谈系统运维负责人，测评是否选择符合国家有关规定的安全服务单位进行相关的安全服务工作。 |

10、安全运维管理测评及工具测试

安全运维管理测评将通过访谈和检查的形式评测系统运维管理过程中的安全控制情况。主要涉及安全主管人员、安全管理人员、各类运维人员、各类管理制度、操作规程文件、执行过程记录等

对象。在内容上，系统运维管理测评实施过程涉及 14 个工作单元，具体如下表：

| 序号 | 安全子类 | 测评指标描述 |
|---|---|---|
| 1 | 环境管理 | 通过访谈物理安全负责人，检查机房安全管理制度，机房和办公环境等过程，测评是否采取必要的措施对机房的出入控制以及办公环境的人员行为等方面进行安全管理。 |
| 2 | 资产管理 | 通过访谈资产管理员，检查资产清单，检查系统、网络设备等过程，测评是否采取必要的措施对系统的资产进行分类标识管理。 |
| 3 | 介质管理 | 通过访谈资产管理员，检查介质管理记录和各类介质等过程，测评是否采取必要的措施对介质存放环境、使用、维护和销毁等方面进行管理。 |
| 4 | 设备维护管理 | 通过访谈资产管理员、系统管理员，检查设备使用管理文档和设备操作规程等过程，测评是否采取必要的措施确保设备在使用、维护和销毁等过程安全。 |
| 5 | 漏洞和风险管理 | 通过访谈安全主管、系统管理员，检查系统安全管理制度、系统审计日志和系统漏洞扫描报告等过程，测评是否采取必要的措施对系统的安全配置、系统账户、漏洞扫描和审计日志等方面进行有效的管理。 |
| 6 | 网络和系统安全管理 | 通过访谈安全主管、网络管理员，检查网络安全管理制度、网络审计日志和网络漏洞扫描报告等过程，测评是否采取必要的措施对网络的安全配置、网络用户权限和审计日志等方面进行有效的管理，确保网络安全运行。 |
| 7 | 恶意代码防范管理 | 通过访谈系统运维负责人，检查恶意代码防范管理文档和恶意代码检测记录等过程，测评是否采取必要的措施对恶意代码进行有效管理，确保系统具有恶意代码防范能力。 |
| 8 | 配置管理 | 通过访谈系统运维负责人，核查配置库的建立和维护情况。 |
| 9 | 密码管理 | 通过访谈安全员，测评是否能够确保信息系统中密码算法和密钥的使用符合国家密码管理规定。 |
| 10 | 变更管理 | 通过访谈系统运维负责人，检查变更方案和变更管理制度等过程，测评是否采取必要的措施对系统发生的变更进行有效管理。 |
| 11 | 备份与恢复管理 | 通过访谈系统管理员、网络管理员，检查系统备份管理文档和记录等过程，测评是否采取必要的措施对重要业务信息，系统数据和系统软件进行备份，并确保必要时能够对这些数据有效地恢复。 |
| 12 | 安全事件处置 | 通过访谈系统运维负责人，检查安全事件记录分析文档、安全事件报告和处置管理制度等过程，测评是否采取必要的措施对安全事件进行等级划分和对安全事件的报告、处理过程进行有效的管理。 |
| 13 | 应急预案管理 | 通过访谈系统运维负责人，检查应急响应预案文档等过程，测评是否针对不同安全事件制定相应的应急预案，是否对应急预案展开培训、演练和审查等。 |
| 14 | 外部运维管理 | 通过访谈系统运维负责人，核查外包运维服务商选择和安全相关 |

| | | |
|---|---|---|
| | | 协议的签订情况。 |

11、工具测试

根据工具测试过程管理表单，使用漏洞扫描工具对信息系统的设备进行扫描，扫描结束后，根据目标设备的具体情况，判断漏洞验证的风险程度。

**三、实施流程**

1、测评准备活动：测评准备活动中，投标人主要完成启动测评项目，组建测评项目组；通过收集和分析被测系统的相关资料信息，掌握被测系统的大体情况；并准备测评工具和表单等测评所需的相关资料；

2、方案编制活动：方案编制活动中，投标人主要完成确定测评对象和测评指标，选择测试工具接入点，从而进一步确定测评实施内容，并从已有的测评指导书中选择本次需要用到的测评指导书，最后根据上述情况编制测评方案；

3、现场测评活动：现场测评活动中，投标人在与测评委托单位就测评方案达成一致意见，并进一步确定测评配合人员，完成测评指导书各项测评内容，获取足够的测评证据；

4、分析与报告编制活动：分析与报告编制活动中，测评人员通过分析现场测评获得的测评证据和资料，判定单项测评结果及单元测评结果，进行整体测评和风险分析，形成等级测评结论，并编制测评报告。

# 第四部分 商务要求

**1、 交货地点：**湖南省中西医结合医院（湖南省中医药研究院附属医院）

**2、 服务工期：**自开工之日起，3 周内（含节假日及周末）完成初审，配合投标方整改后，3 周内(含节假日及周末）完成复审。（具体条款以合同商务条款为准。）

**3、 报价要求：**

（1）投标应对网络安全等级保护测评及安全服务项目报总价，人民币报价。报价包含项目执行中的所有费用，院方不再另行支付其他任何费用。

（2）投标总价中不得包含招标文件要求以外的内容，否则在评审时不予核减。投标总价中也不得缺漏招标文件要求的内容，否则评审时将有效投标中该项内容的最高价计入其评审总价。

（3）投标人所报的投标价在合同执行过程中是固定不变的，不得以任何理由予以变更。任何包含价格调整要求的投标被认为是非实质性响应投标而予以拒绝。

**4、 货款支付：**

每完成单个项目验收合格并通过后，支付相应项目等级测评费用 95%；1 年安全服务到期后支付安全服务费用。项目整体完成并通过验收、质保期满且项目交付无任何问题，支付合同总金额的 5%。

**5、 服务要求：**

（1）本次等级测评应满足的原则，投标人应严格依据下列原则和国家等级保护相关标准开展项目实施工作。

①保密原则：对测评的过程数据和结果数据严格保密，未经授权不得泄露给任何单位和个人，不得利用此数据进行任何侵害招标人的行为，否则招标人有权追究投标人的责任；

②标准性原则：测评方案的设计与实施应依据国家等级保护的相关标准进行；

③规范性原则：投标人的工作中的过程和文档，具有很好的规范性，可以便于项目的跟踪和控制；

④可控性原则：测评服务的进度要跟上进度表的安排，保证招标人对于测评工作的可控性；

⑤整体性原则:测评的范围和内容应当整体全面,包括国家等级保护相关要求涉及的各个层面；

⑥最小影响原则：测评工作应尽可能小的影响系统和网络，并在可控范围内；测评工作不能对现有信息系统的的正常运行、业务的正常开展产生任何影响。

（2）本次等级测评的整体要求：

①投标人应详细描述本次信息系统安全等级保护测评的整体实施方案，包括项目概述、等级保

护测评方案、测试过程中需使用测试设备清单、时间安排、阶段性文档提交等；

②投标人应详细描述测评人员的组成、资质及各自职责的划分。投标人应配置有测评资质的专业人员进行本次信息安全等级保护测评工作；

③本次信息系统安全等级保护测评实施过程中所使用到的各种工具软件由投标人推荐，经招标人确认后由投标人提供并在信息系统等级保护测评中使用；

④信息系统安全等级保护测评需要的运行环境（如场地、网络环境等）由招标人提供，投标人应详细描述需要的运行环境的具体要求。

**6、 验收：**

（1）验收内容：HIS 系统等保测评；LIS 系统等保测评；PACS 系统等保测评；EMR 系统等保测评；互联网医院系统等保测评；一年安全服务

（2）验收条件:医院拿到相应系统的（HIS 系统；LIS 系统；PACS 系统；EMR 系统；互联网医院系统）三级安全等级保护证书。

（3）验收方式：分项验收，即每拿到一个系统的三级安全等级保护证书视为该系统等保测评通过验收。