附件1

**2019年信息安全等级保护测评**

**服务项目配置需求**

**一、等级保护测评服务项目技术需求**

（一）项目测评服务需求和技术要求：为了保障四川省妇幼保健院“核心业务系统（HIS系统）、妇幼卫生信息直报系统、出生医学证明管理系统”安全、稳定、可靠、高效的运行，按照国家网络安全等级保护2.0系列标准要求对其进行安全等级保护三级测评。测评内容包括：安全物理环境、安全通信网络、安全区域边界、安全计算环境、安全管理中心、安全管理制度、安全管理机构、安全管理人员、安全建设管理、安全运维管理等方面。通过测评，对照相应安全等级保护要求进行差距分析，排查系统安全漏洞和隐患并分析其风险，制订出整改措施，出具测评报告。

（二）具体内容包括：对四川省妇幼保健院“核心业务系统（HIS系统）、妇幼卫生信息直报系统、出生医学证明管理系统”的安全物理环境、安全通信网络、安全区域边界、安全计算环境、安全管理中心、安全管理制度、安全管理机构、安全管理人员、安全建设管理、安全运维管理共10个层面通过访谈、检查、测评等方法进行初测评，找出差距、安全漏洞和隐患并分析其风险，制订出整改建议报告。

（三）按照《GB/T22240-2008 信息系统安全等级保护定级指南》、《GB/T 22239-2008信息安全技术 信息系统安全等级保护基本要求》等国内相关标准，及初测评的整改意见协助四川省妇幼保健院完成被测信息系统技术方面的安全修复、系统加固等工作。

（四）测评内容包括信息系统技术安全性测评及信息系统管理安全性测评：

1.信息系统技术安全性测评包括但不限于：安全物理环境、安全通信网络、安全区域边界、安全计算环境、安全管理中心。

2.信息系统管理安全测评包括但不限于：安全管理制度、安全管理机构、安全管理人员、安全建设管理、安全运维管理。

3.安全漏洞扫描包括但不限于：应用系统漏洞扫描、应用服务器漏洞扫描、数据库服务器漏洞扫描。

（五）测评具体要求如下：

1.信息系统技术安全性测评

（1）安全物理环境测评

安全物理环境测评应当包含：安全物理环境测评：物理位置选择、物理访问控制、防盗窃和防破坏、防雷击、防火、防水和防潮、防静电、温湿度控制、电力供应、电磁防护等方面。

（2）安全通信网络测评

安全通信网络测评应当包含：网络架构、通信传输、可信验证等方面。

（3）安全区域边界测评

安全区域边界测评应当包含：边界防护、访问控制、入侵防范、恶意代码和垃圾邮件防范、安全审计、可信验证等方面。

（4）安全计算环境测评

安全计算环境测评应当包含：身份鉴别、访问控制、安全审计、入侵防范、恶意代码防范、可信验证、数据完整性、数据保密性、数据备份恢复、剩余信息保护、个人信息保护等方面。

（5）安全管理中心测评

安全管理中心测评应当包含：安全管理中心测评：系统管理、审计管理、安全管理、集中管控等方面。

2.信息系统管理安全测评

（1）安全管理制度测评

安全管理制度测评应当包含：安全策略、管理制度、制定和发布、评审和修订等方面。

（2）安全管理机构测评

安全管理机构测评应当包含：岗位设置、人员配备、授权和审批、沟通和合作、审核和检查等方面。

（3）安全管理人员测评

安全管理人员测评应当包含：人员录用、人员离岗、安全意识教育和培训、外部人员访问管理等方面。

（4）安全建设管理测评

安全建设管理测评应当包含：系统定级和备案、安全方案设计、产品采购和使用、自行软件开发、外包软件开发、工程实施、测试验收、系统交付、等级测评、服务供应商选择等方面。

（5）安全运维管理测评

安全运维管理测评应当包含：环境管理、资产管理、介质管理、设备维护管理、漏洞和风险管理、网络和系统安全管理、恶意代码防范管理、配置管理、密码管理、变更管理、备份与恢复管理、安全事件处置、应急预案管理、外包运维管理等方面。

3.风险分析和评价

依据GB/T 20984-2007《信息安全技术 信息安全风险评估规范》，针对四川省妇幼保健院“核心业务系统（HIS系统）、妇幼卫生信息直报系统、出生医学证明管理系统”采用风险分析方法，分析信息系统测评结果中存在的安全问题可能对信息系统安全造成的影响，并给出发现的安全问题以及风险分析及评价情况。

4.安全漏洞扫描

安全漏洞扫描应当依据GB/T 18336-2015《信息技术 安全技术 信息技术安全性评估准则》、GB/T 20274-2008《信息系统安全保障评估框架》对四川省妇幼保健院“核心业务系统（HIS系统）、妇幼卫生信息直报系统、出生医学证明管理系统”的应用安全漏洞、主机安全漏洞、数据库安全漏洞三个内容进行测评。

（六）实施和保障方案

1.项目进度要求

本项目测评实施要求同步实施、重点先行、阶段性成果展现相结合。

具体实现进度要求如下：

本次信息系统安全等级保护测评服务工作分为：测评准备、方案编制、现场测评、问题整改、回归测评、报告编制等几个阶段。

（1）第一阶段：

组建项目组，制定信息安全测评项目计划书、测评实施方案以及人员安全培训计划，并提交四川省妇幼保健院审核。

（2）第二阶段：

进行现场测评，同时对四川省妇幼保健院信息安全相关管理和技术人员进行安全技术培训。初次测评完成后，提交初评的整改意见报告。

（3）第三阶段：

协助四川省妇幼保健院针对测评过程中发现的安全问题进行技术整改加固工作，并进行整改后的回归测评。

（4）第四阶段：

整理测评结果，向四川省妇幼保健院提交被测信息系统安全等级保护测评报告以及相应文档。

2.项目实施要求

依据国家各项相关标准法规和四川省妇幼保健院现有的规范、制度，同时结合项目实际需要，对信息安全等级保护项目工作中的定级、备案、测评（包括测评范围、测评方法等）、整改（包括整改方法、范围等）过程中，所需的产品、技术、制度、流程、建设要求和实施规范等方面，提供咨询、测评、整改建议以及整个建设过程的监督和管理等服务。所提供的整体方案需包括技术方案和实施方案。技术方案包括整体流程、技术方法和服务方案设计等，需要对每项技术方法的应用位置进行详细描述，对系统进行详细的测评，发现系统不足，明确安全风险隐患和差距，提出整改意见，协助四川省妇幼保健院信息安全管理人员进行整改；实施方案包括人员组织、时间安排、阶段性文档提交、验收标准、质量保证和风险规避措施等，需要明确每项工作的时间安排、操作时间和操作人员。投标人负责提供的服务内容至少应包括，但不限于以下各项：

（1）服务提供商在信息安全等级保护测评和风险评估前应制定详细的技术方案，包括信息安全等级保护测评项目计划书、测评实施方案以及人员安全培训计划等，并提交四川省妇幼保健院审核。

（2）信息安全等级保护测评包括但不限于以下对象：网络结构、网络服务、主机系统、存储备份系统、数据库、中间件、应用系统、数据安全、安全系统、系统安全策略等。

（3）服务提供商应描述测评服务的技术方案，包括准备工作、技术措施、人员安排、时间进度、可能对系统造成的影响等。

（4）安全测评工作应尽量选择在非业务繁忙时段进行，将对被测系统可能带来的影响减至最小。

（5）信息安全等级保护测评完后，协助被测评单位整理备案材料和进行安全主管部门备案工作。

（6）服务提供商应书面承诺能够积极与四川省妇幼保健院协作，共同完成本项目的测评工作，项目实施过程中出现问题不得互相推诿，双方应主动进行沟通，并及时解决问题，确保项目顺利实施。

3.项目管理要求

对项目进行科学严格的管理，通过系统计划、有序组织、科学指导和有效控制，促进项目全面顺利实施，投标人必须提供完整的项目管理方案，项目的方案设计与具体实施应满足以下原则：

（1）最小影响原则：工作应尽可能小的影响系统和网络的正常运行，不能对网络的运行和业务的正常运行产生显著影响（包括系统性能明显下降、网络拥塞、服务中断）；

（2）标准性原则：服务方案的设计与实施应依据国家网络安全等级保护2.0相关标准进行；

（3）规范性原则：服务提供商工作中的过程和文档，应具有较好的规范性，便于项目的跟踪和控制；

（4）可控性原则：方法和过程要在双方认可的范围之内，安全服务的进度要按照进度表安排实施，保证四川省妇幼保健院对于服务工作的可控性；

（5）整体性原则：评估内容应当整体全面，包括安全涉及的各个层面，避免由于遗漏造成未来的安全隐患；

（6）保密原则：对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采购人的行为，否则四川省妇幼保健院有权追究服务提供商的责任。

服务提供商需根据上述要求，提供项目详细的项目管理方案，并予以详细解释。

4.服务保障与承诺

（1）服务提供商应严格按照测评人员执业守则，按照国家相关法规、规范、标准及制定的测评方案、项目计划书、实施细则进行测评，在保证质量、安全的前提下，确保在项目规定的期限内按期完成。

（2）服务提供商应协助、配合四川省妇幼保健院与上级监管部门、公安机关的沟通协调。在测评过程中和测评完成后，协助、配合四川省妇幼保健院进行相关的信息系统安全整改，确保已定级系统达到等级保护的相关要求，并通过上级监管部门和公安机关的审核验收。

（3）服务提供商应在项目期内向四川省妇幼保健院提供7\*24小时电话咨询服务，必要时上门服务。跟踪信息安全等级保护的最新发展情况，及时告之四川省妇幼保健院，提供相应解决方案及建议，协助其持续符合信息系统信息安全等级保护工作的要求。

（4）服务提供商应在项目实施过程中，对四川省妇幼保健院相关人员进行安全方面的技术培训，明确项目实施的思路、方案、技术路线，提升技术人员的安全意识，可以独立的对信息安全等级保护的国家安全政策和法规进行把握，了解测评整改手段，掌握测评整改方法。

（5）服务提供商应在项目开始前，与四川省妇幼保健院签订保密协议，严格遵守法律法规，对四川省妇幼保健院商业秘密、系统风险信息、项目实施内容及成果信息进行严格保密，未经四川省妇幼保健院同意，严禁将上述内容与任何第三方透露或用于其他商业用途，并承担由此产生的一切损失。

**二、评分办法：**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 序号 | 评分因素及权重 | 分值 | 评分标准 | 说 明 |
| 1 | 报价20% | 20分 | 价格得分=（评标基准价/投标报价）×20评标基准价指满足招标文件要求且投标价格最低的投标报价）。1、根据《政府采购促进中小企业发展暂行办法》（财库[2011]181号）的规定，对小型和微型企业产品的价格给予6%的价格扣除，用扣除后的价格参与评审。2、参加政府采购活动的中小企业应当提供《中小企业声明函》原件。 |  |
| 2 | 项目实施方案10% | 10分 | 信息系统安全测评方案的完整性、可行性、技术性等进行横向比较评分：优秀的（完全响应并优于比选文件的技术要求），得10分；良好的（完全响应比选文件的技术要求），得8分；一般的（基本响应比选文件的技术要求），得6分；较差的（测评技术方案不合理，未响应比选文件的技术要求），得5分及以下。 | 照抄比选文件技术要求不得分。 |
| 3 | 项目团队情况33% | 33分 | 一、项目总测评师（10分）：总测评师具有省级及以上人力资源部门颁发的高级工程师证书、中国信息安全认证中心颁发的信息安全服务资质认证审查员（ISCCC）证书、公安部信息安全等级保护评估中心颁发的信息安全等级保护高级测评工程师证书、中国信息安全认证中心（ISCCC）颁发的信息安全保障人员认证（注册方向：安全软件专业）证书等证书，每具备一个得2.5分，最高得10分；没有的得0分。二、项目测评工程师（23分）：1、测评工程师具有公安部信息安全等级保护评估中心颁发的信息安全等级保护高级测评工程师证书，每有一人得2.5分，最多得10分；没有的得0分。2、测评工程师具有中国信息安全认证中心（ISCCC）颁发的信息安全保障人员认证（注册方向：安全软件专业）证书，每有一人得2分，最多得8分；没有的得0分。3、测评工程师具有中国信息安全认证中心颁发的信息安全服务资质认证审查员（ISCCC）证书，每有一人得1.25分，最多得5分；没有的得0分。 | 提供人员资质证书复印件（加盖公章，原件备查）。 |
| 4 | 服务提供商履约能力32% | 32分 | 1、服务提供商拥有中国信息安全认证中心（ISCCC）颁发的信息安全风险评估一级资质的得10分；二级资质的得5分；没有的得0分。2、服务提供商拥有中国信息安全认证中心（ISCCC）颁发的信息安全运维服务一级资质的得10分；二级资质的得5分；没有的得0分。3、服务提供商近三年（2017年-2019年）从事过医疗卫生行业信息安全等级保护测评（三级及以上）项目案例，每个得2分，最高得12分；没有的得0分（需提供合同复印件或项目验收书）。 | 同一案例不重复计分。提供有效证明文件复印件并加盖鲜章，否则不计分。 |
| 5 | 本地化服务3% | 3分 | 服务提供商在本地有注册登记的检测实验室或分支机构的得3分 。 | 提供证明材料，加盖公章，原件备查。 |
| 6 | 投标文件规范性2% | 2分 | 投标文件制作规范，没有细微偏差情形的得1分；有一项细微偏差扣0.5分，直至该项分值扣完为止。 |  |

附件2

采购文件书装订顺序

1、封面（公司、项目、联系人、联系方式）

2、目录

3、报价一览表

4、 企业营业执照副本或者事业单位法人证书副本（复印件）

5、组织机构代码证、税务登记证（复印件）（或三证合一）。

6、法定代表人授权书、暨经办人授权书，法人、经办人身份证（复印件）

7、如有企业管理体系认证（考核），请提供的有效证明文件的复印或扫描件，质量管理体系认证包括FDA、CE、ISO等认证（提供中文翻译复印件）,如具有信息系统项目管理师、IT服务项目经理、国家注册信息安全专业人员、国家信息安全保障人员、网络工程师、RHCE系统工程师资质请提供有效证明文件或扫描件

8、设计规范或标准

9、售后服务承诺书

10、业绩证明文件（近一年用户名单及联系人与联系方式及合同复印件或近三个月内送货复印件，格式见附件3）。

11、封底

**注：请务必按以上顺序装订资料，如有非中文资料，请同时提供中文翻译件。**

附件3

四川省妇幼保健院信息安全等级保护测评项目报价一览表

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 序号 | 项目名称 | 数量 | 单价（万元） | 金额（万元） | 备注 |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  | **合计** |  |  |  |  |

注：1.报价应是最终用户验收合格后的总价，税费、采购文件规定的其它费用。

2.“报价一览表”为多页的，每页均需由法定代表人或授权代表签字并盖投标人印章。

3.“报价一览表”需单独密封。

供应商名称（盖章）：

法定代表人或授权代表（签字）： 联系方式：

日期：

附件4

反商业贿赂承诺书

为维护卫生行业的整体形象，保证药品、医疗器械、仪器设备、物资、基建工程招投标工作以及药品、试剂销售等工作的合法开展，维护贵院医疗、管理工作的正常秩序，保障广大患者的健康和利益，本厂家、商家、公司特郑重承诺如下：

一、严格按照《招标投标法》、《药品管理法》、《反不正当竞争法》等有关法律、法规、规章、政策的规定，规范本厂家、商家、公司的药品、医疗器械、设备、物资、基建工程竞标工作以及药品准入贵院以后的销售等工作，保证做到合法竞标、正当竞争、廉洁经营。

二、本厂家、商家、公司保证在药品、医疗器械、设备、物资、基建工程竞标工作及药品、试剂销售等工作中承诺做到：

1、不与其他投标人相互串通投标报价，损害贵院的合法权益；

2、不与招标人串通投标，损害国家利益、社会公共利益或他人的合法权益；

3、不以向招标人或者评标委员会成员行贿的手段谋取中标；

4、竞标报价不违反相关法律的规定，也不以他人名义投标或者以其他方式弄虚作假，骗取中标；

5、保证不以其他任何方式扰乱贵院的招标工作；

6、保证不在药品销售、医疗器械、设备、物资、基建工程竞标中采取账外暗中给予回扣的手段腐蚀、贿赂医护、药剂人员、干部等其他相关人员；

7、保证不以任何名义包括以宣传费、临床促销费、开单费、处方费、广告费、免费度假、考察旅游、房屋装修等任何名义给予贵院采购人员、药剂人员、医护人员、干部等有关人员以财物或者其他利益；

8、保证不让贵院临床科室、药剂部门以及有关人员登记、统计医生处方或为此提供方便，干扰贵院的正常工作秩序；

9、保证不以其他任何不正当竞争手段推销药品、医疗器械、设备、物资。

三、本厂家、商家、公司保证竭力维护贵院的声誉，不做任何有损贵院形象的事情。

四、本厂家、商家、公司保证加强对竞标、促销等工作的领导、监督和检查；加强对本厂家、商家、公司工作人员进行相关法律、法规、规章、政策等的教育工作，切实要求本厂家、商家、公司相关工作人员不得采取各类回扣手段腐蚀、贿赂采购、药剂、医护、干部等相关人员。

五、对本厂家、商家、公司及本厂家、商家、公司工作人员采取以上手段竞标、促销等，干扰贵院正常工作秩序，损害贵院形象的，本厂家、商家、公司保证：

1、对尚处在竞标阶段的，贵院有权取消本厂家、商家、公司的竞标资格；已经中标的，贵院有权取消中标；对已经获得准入资格的，贵院有权随时取消本厂家、商家、公司的准入资格；

2、对本厂家、商家、公司相关工作人员作出严肃处理；

3、对由于本厂家、商家、公司或本厂家、商家、公司工作人员的上述行为给贵院造成经济或名誉损失的，由本厂家、商家、公司负责，并愿意承担全部民事赔偿责任。

六、 采购物资名称：

本《承诺书》一式伍份（一份由承诺人自存；一份随竞价书传递）

承诺企业名称（公章）

法人代表或委托代理人（承诺人）