# 采购内容及要求

**一、项目概述**

为贯彻落实国家信息安全等级保护制度，瑞安市人民医院决定对本单位开展信息安全等级保护测评工作，并进一步完善瑞安市人民医院信息系统安全管理体系和技术防护体系、增强信息安全保护意识、明确信息安全保障重点、落实信息安全责任等工作提供依据，切实提高系统信息安全防护能力。

**二、信息系统清单：**

1.具体需要测评的信息系统如下：

|  |  |  |
| --- | --- | --- |
| **序号** | **系统名称** | 安全保护等级 |
| 1 | 面向患者的业务系统 | 三级 |
| 2 | 基础支撑系统 | 三级 |

**本项目采购预算为9万元。**

**三、测评依据**

供应商应依据国家等级保护相关标准开展工作，依据标准包括但不限于如下国家标准：

GB/T 22239-2019《信息安全技术 网络安全等级保护基本要求》

GB/T 28448-2019《信息安全技术 网络安全等级保护测评要求》

四、服务内容要求

（一）测评内容服务

根据《信息系统安全等级保护定级指南》和国家网络安全等级保护2.0相关标准，供应商对本单位的信息系统安全等级保护测评的内容包括但不限于以下内容：

从业务信息安全性和系统服务保障安全要求两个方面分析信息系统的业务和服务安全保护级别，确定信息系统的安全等级。通过对被测系统的详细了解，至少应包含信息系统调查、定级对象分析、定级要素分析等，确保信息系统定级备案的合理性，最后完成信息系统《等级保护定级报告》，并协助完成报备等相关工作。

基于《信息系统安全等级保护基本要求》（GB/T22239-2019）的等级保护测评服务（包括物理安全、网络安全、主机系统安全、应用安全和数据安全、安全管理机构、安全管理制度、人员安全管理、系统建设管理和系统运维管理等十个方面的安全测评），提交符合公安部门要求的信息安全保护等级测评报告等有关材料，并协助完成备案工作。

（二）渗透测试服务

对项目内系统进行渗透测试，模拟黑客攻击，在甲方的授权和监督下对应用、系统和网络进行非破坏性质的攻击性测试，发现系统中存在的安全隐患，提出解决问题的建议措施，并协助进行修复。

（三）等保安全保障方案设计服务

根据等级保护差距测评报告，针对存在的安全隐患以及未落实的安全措施制订安全整改方案，明确整改的目标、项目和进度，拟定信息安全标准与规范。

（四）安全增值服务

提供1年的安全专家咨询服务、安全策略与规范拟定服务、安全制度建设服务。

四、技术服务要求

（一）测评应满足的原则

1.标准性原则：服务方案的设计与实施应依据国家等级保护的相关标准进行。

2.规范性原则：服务工作过程中的文档，具有良好的规范性，便于项目的跟踪和控制。

3.可控性原则：服务工作的进度要严格进度表的安排。

4.整体性原则：服务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。

5.最小影响原则：服务工作对系统和网络的影响必须在可控范围内，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。

（二）等级保护测评要求

1.供应商应详细描述本次等级保护测评的整体实施方案，包括项目概述、等保测评方案、项目实施方案、测试过程中需使用测试设备清单、时间安排、阶段性文档提交和验收标准等。

2.供应商应详细描述测评人员的组成、资质及各自职责的划分。供应商应安排专职项目经理和项目实施负责人负责本次项目的实施，供应商应配置有经验的测评人员进行本次等级保护测评工作。

3. 本次等级保护测评实施过程中所使用到的各种工具软件由供应商推荐，经采购人确认后由供应商提供并在测评中使用。在投标文件中应详细描述所使用的安全测评工具（软硬件型号、功能和性能描述）、使用的方式和时间、对环境和平台的要求以及使用可能对系统造成的风险等。在等级保护测评过程中，应采用询问、检查、测试、工具扫描等多种手段组合的方式。等保测评工具原厂商应该是公安部认可的信息安全等级保护测评工具研发单位。

4.对于在测评过程中采用的测评方法、测评所使用的工具、测评所覆盖的各方面，需要符合信息安全等级保护主管部门要求。

5.安全测评工具软件运行可能需要的硬件平台（如笔记本电脑、PC、工作站等）和操作系统软件等由供应商推荐，经采购人确认后由供应商提供并在测评中使用。

6.安全测评需要的运行环境（如场地、网络环境等）由采购人提供，供应商应详细描述需要的运行环境的具体要求。安全调查和测评的过程中，供应商如需采购人人员配合，供应商需要详细描述需要配合的内容。如需要采购人人员协助完成各种表单，需要详细描述表单的名称、功能及主要表项等等，并由供应商给出具体示例。采购人有权利拒绝提供任何未事先提出的配合要求，由此产生的损失由供应商负全责。

7.安全测评应按照分层的原则，包括但不限于以下对象：物理环境、网络结构、网络服务、主机系统、数据库系统、应用系统、安全相关人员、处理流程、安全管理制度、安全策略等。

8.供应商应提供本项目的测评方案，包括技术部分和实施部分。技术部分包括整体流程、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，技术方案中应详细描述本次测评采用的测评方式及标准、漏洞测试和应用分析的方法；

9.实施部分包括人员组织、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。安全调查和测评过程中，如需使用安全工具，请在实施方案中详细描述所使用的安全工具（软硬件型号、功能和性能描述）、使用的方式和时间、对环境和平台的要求等。

10.供应商应详细描述安全调查和测评的组织方式，包括组成的人员及分工、测评的过程组织、实施时间安排、测评方式所遵循的标准等。

11.项目完成后必须提交完整的技术文档、测评报告、整改建议等，并负责对相关人员进行培训。

（三）项目实施要求

1.供应商应保证投标项目在采购人条件成熟时应立即开展实施；

2.供应商在项目实施过程中应服从采购人的统一领导和协调，采购人有权裁决供应商的责任范围，供应商必须执行，在采购人限定的时间内解决问题。如果供应商不能按时完成评估内容，采购人有权中止项目、索赔或拒付款项；

3.供应商应在项目现场实施周期内，供应商必须为本项目成立等级保护测评小组，安排包括项目经理和核心技术人员的现场驻场服务；

4.供应商需根据自己的工程实施经验结合采购人的实际需求进一步细化和完善工作任务书，作为工程实施的指导性文件；

5.供应商应根据采购人工作需求、进度要求、实际情况制定详细的项目实施管理规范和项目实施计划，对工程目标、工作任务、阶段性工作、项目组织机构、职责分工、项目进度、质量控制等内容进行详细的说明，以确保工程实施按时保质的完成；

6.供应商应负责配合采购人制定相关验收标准，并完成工程实施等验收工作。

7.在整改过程中，集成服务商整改加固过程需本项目供应商全程驻场配合并进行符合性复测。

8.项目验收完成后，要求提供为期两年的技术咨询服务，以保证项目正常运行。

9.项目执行周期要求合同签订后90个日历天内完成。

（四）测评报告要求

供应商应对采购人的各个信息系统进行等级保护测评，形成相应的报告。

1.《测评结果报告》

安全评估报告即等级保护差距测评报告主要体现各系统针对物理安全、网络安全、主机系统安全、应用安全和数据安全、安全管理制度、安全管理机构、人员安全管理、系统建设管理和系统运维管理等十个方面的安全差距，内容包括：信息系统现状、信息系统安全测评的方法、信息系统运行环境测评、等级测评内容。差距测评报告无需提供等级保护测评结论。

2.供应商在测评完成后，出具符合信息安全等级保护主管部门要求的信息系统安全等级保护测评符合性报告，整改加固后进行符合性性复测；报告格式及内容应完全依据浙江省网警总队公布的《信息系统安全等级测评报告模板》，内容包括：信息系统现状、信息系统安全测评的方法、信息系统运行环境测评、等级测评内容、剩余风险分析与评价、等级评测结论。

3.供应商协助用户方完成等级保护要求各项管理制度；

4.对不符合信息安全等级保护有关管理规范和技术标准的，供应商出具可行的信息系统整改建议，并指导用户方完成整改；

五、保密要求

（一）对服务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采购人的行为，否则采购人有权追究供应商的责任；

（二）对涉及客户的检查项目、资料、检查过程和结果以及客户的知识产权、所有权等其它信息采取保密措施；

（三）在接收客户的检查项目时，应对检查项目加强监管，防止泄密。信息安全等级保护测评之前必须签订保密协议。所有检查项目，不经用户同意，不得向与检查无关人员展示；

（四）所有检查过程均对外保密，与检查无关人员未经采购人批准，不得擅自进入检查现场；

（五）在未经许可的情况下与检查无关的人员不得接触被检查项目及相关资料，不得参与检查和编制检查报告；

（六）出具的检查报告应为采购人保密，未经采购人授权，不得将检查报告转交他人，不得擅自公布检查结果；

（七）当有关人员要求用电话、图文传真或其它方式传送检查结果时，应有采购人正式的书面委托并证实相关通讯方式可靠后方可执行；

（八）不得向无关人员泄露任何有关采购人资料和检查结果，检查结果只能通过相关程序及约定的告知方式通知相应业务单位和个人；

（九）对接触客户检查项目、资料及其它相关信息的人员应履行为采购人保护所有权的义务，不得利用采购人的有关知识产权为己牟利。

**评分标准**

**综合评分（100分）**

21.1本次评审采用综合评分法，总分为100分。

21.2评审时，磋商小组认为供应商的报价明显低于其他通过符合性审查供应商的报价，有可能影响产品质量或者不能诚信履约的，应当要求其在评审现场合理的时间内提供书面说明，必要时提交相关证明材料，供应商不能证明其报价合理性的，磋商小组应当将其作为无效投标处理。

21.3评审因素

商务技术评分由评委成员按下列评分细则中的评分项目进行统一评判打分，并记名。评标委员会对各投标供应商评分的算术平均值为各投标供应商的商务技术分最终得分（小数点后按四舍五入保留2位）。

**1、商务技术分的评定（80分）**

|  |  |  |  |
| --- | --- | --- | --- |
| 序号 | 项目 | 分值 | 评审要求及打分说明 |
| 1 | 技术方案 | 10分 | 针对本项目的方案设计10分。响应磋商文件整体需求，针对本项目编制详细的项目技术方案设计，设计的技术方案全面、合理、针对性强。方案全面、合理的7-10分；较全面、较合理的4-7分；方案不全面、不合理的得0-4分；未提供该方案不得分。 |
| 2 | 实施方案 | 10分 | 针对本项目的项目实施计划安排与现场情况的合理性，根据方案的科学性、实用性、有效性、可操作性打分，满分10分。方案完整细致，合理可行，在全部满足项目需求的前提下，能提供多种服务方式，得7-10分；方案较完整细致，基本合理可行，基本满足项目需求，得4-7分；方案简单，可行性较差，部分满足项目需求，得0-4分；未提供该方案不得分。 |
| 3 | 咨询服务及技术支持方案 | 7分 | 投标供应商应针对测评完成后，在系统安全整改阶段提供咨询服务及技术支持方案及承诺，满分7分。  方案完整细致，合理可行，在全部满足项目需求的前提下，能提供多种服务方式，得5-7分；方案较完整细致，基本合理可行，基本满足项目需求，得3-5分；方案简单，可行性较差，部分满足项目需求，得0-3分；未提供该方案不得分。 |
| 4 | 公司资信 | 17分 | 1.具有信息系统安全风险评估二级及以上服务资质得3分；  2.具有信息系统安全运维二级及以上资质证书得3分。  3.具有信息安全应急处理二级及以上资质证书得3分。  4.在国家密码管理局公布的《商用密码应用安全性评估试点机构目录》名单范围内得4分。  5.具有中国合格评定国家认可委（CNAS）颁发的实验室或检验机构认可证书得4分；  注∶投标供应商须提供相关资质证书复印件并加盖公章，否则不予认可。 |
| 5 | 项目业绩 | 10分 | 1.投标供应商提供2020年1月1日至今所承担的类似项目业绩，以合同签订时间为准的单项合同：完成过包含系统信息安全等级保护测评的项目，每有一个得2分，满分6分；  2.提供自2020年1月1日（以合同签订时间为准）至今承担的网络安全检查项目或风险评估业绩案例，每提供一个项目案例得2分，满分4分；  注∶1、投标供应商业续需提供合同复印件（内容至少包括合同首页、检测内容页、金额页、签字盖章页）并加盖公章;  2、同一个业绩只能计一次，不能重复计分。 |
| 6 | 项目人员实力 | 20分 | 1、项目负责人  项目负责人同时具有高级信息安全等级保护测评师证书资质、计算机类正高级工程师资格、信息系统项目管理师、注册信息安全专业人员CISP 认证证书，符合一项得1分，符合两项得3分，全部符合得满分6分。  2.项目团队   1. 确保项目组人员在5人及以上（含驻场人员1名），符合要求4分，不符合0分。 2. 项目组成员中具备商用密码应用安全性评估证书，符合要求2分，满分2分。 3. 项目组成员每具有一个CISP或信息安全等级测评证书（中级及以上）的得2分，满分8分；   注∶1、上述人员须提供相关资质证书等证明文件复印件并加盖公章，否则不予认可；  2、同一人员具有多个证书的，不重复计分（按个人最高分计算）；须提供以上人员开标截止日近6个月内任意一个月的社保证明。 |
| 7 | 售后服务和应对能力 | 6分 | 1.按照磋商文件要求提供售后服务方案，方案完整性以及对整体需求的符合承诺情况的得0-3分；  2.拥有专业信息安全防护评估软件，提供知识产权证明得3分。 |

2、 **商务（价格）评分（20分）**：

满足采购文件要求且投标价格最低的投标报价为评标基准价。

1） 有效投标供应商的投标报价等于评标基准价时其价格分为满分20分；

2） 其他投标供应商的价格分按以下公式计算：

投标报价得分=（评标基准价/投标供应商投标价）× 价格权值 ×100（四舍五入，保留小数点后2位）

3、其他

评分时保留小数点后2位小数，计算评分值时保留小数点后2位小数，由磋商小组当场统一计算。

磋商响应供应商的最终总得分为技术、商务、报价三部分得分的总和。

**报价是成交的一个重要因素，但最低报价不是成交的唯一依据。**

21.4 磋商文件没有规定的评审标准不作为评审依据。

21.5磋商小组成员独立对每个有效响应的文件进行评价、打分，所有磋商小组成员的打分平均值为每个供应商的得分。

**合同模板**

**网络安全等级保护测评**

**技术服务合同**

甲方： 瑞安市人民医院

地址： 瑞安市万松路108号

经办人： 卢建继

电话：15058321616

乙方：

地址：

经办人：

电话：

依据《中华人民共和国民法典》的规定，甲乙双方本着平等互利的原则，在友好协商的基础上，就对甲方的基础支撑系统、面相患者服务信息系统等开展安全等级保护测评签订本技术服务合同。

1. **测评服务的内容**

根据甲方委托，乙方就甲方指定的信息系统（本合同第5条所列的信息系统）安全等级保护测评项目提供以下技术服务：

1. 基于《信息安全技术 网络安全等级保护基本要求》（GB/T22239-2019）的对应等级和应用场景（以下选择）的测评服务，并提交反映系统安全现状的系统安全保护等级测评报告。

■安全通用要求

□云计算安全扩展要求

□移动互联网安全扩展要求

□物联网安全扩展要求

□工业控制系统扩展要求

□大数据可参考安全控制要求

1. 现场测评完成后的整改建议服务。
2. **测评服务依据**

依据国家等级保护相关标准开展工作，依据标准包括但不限于如下国家标准：

* GB/T 22239-2019 信息安全技术 网络安全等级保护基本要求
* GB/T 28448-2019 信息安全技术 网络安全等级保护测评要求

1. **工作质量要求**

为了保证本次项目的品质和质量，乙方承诺：

1. 根据标准性、规范性、可控性、整体性、最小影响性及保密性原则，做到守时、保质；
2. 指派测评经验丰富的测评师团队，结合技术领先、结论可靠的测评工具为甲方作全面的等级保护测评。承诺测评过程按照国家标准进行，并保证对客户的资料严格保密；
3. 在甲方指定的地点进行现场测评工作，在测评期间和测评结束后，归还甲方借阅材料；
4. 在关键测评内容实施前（如扫描或工具测试），应和甲方充分沟通和协商，并制定详细的实施方案。
5. **工作条件和协作事项**
6. 甲方应根据乙方的要求予以项目相关配合，包括提供相关资料、协调相关人员、提供必要的工作环境等。
7. 自乙方填报等级测评项目登记管理系统审核通过之日起 一年内（不包含用户整改时间），应按照双方商定的工作要求（包括进度、质量等）完成本合同工作。
8. 项目结束后，乙方不得利用项目过程中获取的资源从事有损于甲方名誉、利益的活动。
9. **合同价格**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 系统名称 | 安全等级 | 单价 | 合计 | 备注 |
| 基础支撑系统 | 第三级 |  |  | 复测 |
| 面相患者的业务系统 | 第三级 |  |  | 复测 |

本合同总价为人民币 元整（大写： ），包括乙方正确、完全地履行本合同服务所需的全部成本及税费。除本合同另有明确规定外，上述合同价格在本合同期间保持不变。

1. **付款方式和付款比例**
2. 甲方应以汇款方式（人民币为支付货币）向乙方以下指定账户支付合同价款：

|  |  |  |
| --- | --- | --- |
| 收款账户 | 户名 |  |
| 开户行 |  |
| 账号 |  |

1. 甲方应按下述规定安排付款：
2. 合同签订生效后并在收到发票的40个工作日内，甲方向乙方支付合同总额的50%，即人民币 （￥ ）。
3. 乙方出具网络安全等级保护测评报告。甲方在收到发票的40个工作日内支付合同总价50%，即人民币 （￥ ）。
4. 乙方承诺在每次付款前，依据甲方提供的如下相关信息开具等同付款金额的税务正式发票给甲方。

|  |  |  |
| --- | --- | --- |
| √增值税普通发票 □增值税专用发票 | | |
| 开票信息 | 单位名称 |  |
| 税号（信用统一代码） |  |
| 地址及电话 |  |
| 开户行及账号 |  |

1. **技术资料或成果输出**

乙方应向甲方提供以下技术资料或成果。上述技术资料的费用应包括在合同总价中，如果技术资料不完整或丢失，甲方应通过书面方式说明原因向乙方提出申请，乙方同意后提供。

* 网络安全等级保护测评报告纸质版（本报告一式三份，一份提交甲方、一份提交受理备案的公安机关、一份由乙方留存）

1. **保密要求**

双方确定因履行本合同应遵守的保密义务具体见附件1。

1. **不可抗力**
2. 本条所述的“不可抗力”是指无法控制、不可预见，并且通常情况下不可避免和克服的事件，包括但不限于：战争、严重火灾、水灾、台风、地震以及双方同意成为不可抗力的其他事件。如果由于不可抗力致使本合同任何一方无法按时履行合同义务，则在受不可抗力影响的时间和范围内双方有权中止对其义务的履行。
3. 发生不可抗力事件时，受不可抗力影响的一方应尽快以书面形式将不可抗力的情况和原因通知另一方。同时必须在不可抗力发生后10日内，以挂号信形式递交有关公证机关的证明。在任何情况下，如果不可抗力事件持续超过90天，则任何一方有权在向对方发出终止通知后终止本合同。
4. **提前终止**
5. 除本合同另有规定外，在发生以下情况时，甲方有权书面通知乙方后终止合同：乙方未履行合同规定的义务并且在接到甲方通知后30天内或甲方同意的更长一段时间内仍不予补救或补救未成；
6. 如果甲方根据第10条第1）款规定终止了合同，则甲方有权：要求乙方退还已支付的未履行部分合同价款；
7. 发生以下情况时，任何一方有权在书面通知另一方后终止合同：
   1. 一方破产或无清偿能力；
   2. 因本条而终止时，乙方仅有权就其在终止之前已履行的服务获得付款。
8. 不论本合同因何种原因而终止均不免除任何一方根据合同规定在终止后仍应履行的其他义务。不论本合同因何种原因终止，乙方未履行部分对应的费用应退还甲方。
9. **违约责任**

双方确定，按以下约定承担各自的违约责任：

1. 乙方违反本合同第4条第二点约定，应当每延迟一天，乙方向甲方按合同总价的0.1％支付违约金，上述违约金总额最多不超过合同总价的10%。
2. 甲方违反本合同第6条第二点约定，应当每延迟一天，甲方向乙方按合同总价的0.1％支付违约金，上述违约金总额最多不超过合同总价的10%。
3. **合同文件的处理**
4. 任何一方不得将本合同、合同的有关条款或在履行本合同过程中所获得其他有关信息透露给第三方。
5. 未经甲方事先同意，除非为履行本合同所用，乙方不得将在合同中涉及的资料用作其他目的。
6. **争议解决**
7. 甲乙双方在执行本合同所发生的一切争执和争议，都可及时友好协商解决；若协商不成，双方可以直接向瑞安市人民法院提起诉讼。
8. 本合同按照中华人民共和国的法律进行解释。

**14、信息对外公布条件**

甲乙双方确认，因法律、法规、国家政策规定等原因必须透露对方保密信息的，在不禁止的情况下，应事先以书面形式通知对方，并且尽力为对方的保密信息提供保护。

**15、其他**

1. 合同未经双方同意不作修改，任何对合同条款的变更或修改均须以双方签订书面修改书的形式进行。
2. 本合同受中国法律管辖并依其进行解释。
3. 未经对方同意，任何一方均不得将其在本合同下的权利和义务转让给其它第三方。
4. 任何一方向对方提出的函电通知或要求，在取得对方人员和或通讯设施接收确认后，即被认为已经被对方正式接收。
5. 本合同的附件是本合同不可分割的一部分，具有与合同同等的法律效力。如果附件与合同条款有冲突，则应以合同条款为准。
6. 本合同经双方授权代表签字、盖章后生效：
7. 本合同正本一式伍份，甲乙双方各执两份，另一份提交浙江省网络安全等级保护工作领导小组办公室备案，具有同等的法律效力。

甲方（盖章）： 乙方（盖章）：

授权代表（签字）： 授权代表（签字）：

日期： 日期：

**保密协议**

甲方： 瑞安市人民医院

乙方：

鉴于乙方对甲方的 基础支撑系统、面相患者的业务系统开展安全等级保护测评工作，在测评工作过程中，双方能够接触或从对方处获得资料、文档和相关业务数据等保密信息，为确保对双方的保密信息进行有效保护，保障各类信息的安全，体现测评工作的诚实性，现甲乙双方经友好协商，达成本协议：

**一、本协议所指保密信息**

1、甲方的保密信息：甲方信息系统的相关信息、主合同服务范围内的工作成果等。

2、乙方的保密信息：乙方的工作方式、原理，以及竞争性技术、主合同服务范围内的工作成果等。

**二、保密期限**

本协议保密期限不论主合同是否变更、解除、终止，长期有效。

**三、涉密人员**

双方参与该测评项目的所有项目人员。

**四、测评过程的保密**

1、乙方所有测评过程均需对外保密，与测评无关的人员未经甲方批准，不得擅入测评区域。

2、凡与测评无关的人员不得接触被检物品及相关文件资料，不得参与测评报告的编制。

3、与甲方系统测评相关的废弃资料应由乙方测评人员负责统一销毁，不得随意丢弃。

4、在抽样测评时，乙方应采取有效措施确保测评对象的保密性。

5、甲方及其参与测评项目的所有人员对于在测评过程中获悉的乙方的工作方式、原理、竞争性技术及其他相关资料均应负责保密。

**五、测评结果的保密**

1、乙方出具的所有测评结果只对甲方及其主管部门提供。乙方所有接触测评结果的人员均应为甲方保密，未经甲方许可，不得擅自向第三方泄露或公布测评结果。甲方的测评报告应由甲方单位负责人或其授权代表领取，未经甲方书面许可，乙方不得委托第三方转交。

2、对留存在乙方存档的所有测评报告副本、原始记录和甲方相关的技术资料，由乙方业务管理部门妥善保管，严格按照乙方《文件控制程序》执行调阅。

3、当甲方要求用电话、图文传真、电子邮件或其它方式传送测评结果时，应由乙方业务管理部门在取得甲方书面许可并明确接受方身份后，在采取一定保密措施（如设置密码、口令等）的基础上予以传送。

**六、违约责任**

任何一方如向第三方泄密，则应赔偿对方因泄密所造成的经济损失，直至追究泄密方的法律责任。

**七、**本协议在履行过程中如发生争议，双方应友好协商解决。协商不成的，则任何一方可将争议提交甲方所在地人民法院诉讼解决。

**八、**本协议未尽事宜，双方可另行协商签订补充协议。

**九、**本协议自双方签字盖章之日起生效。本协议一式贰份，双方各执壹份，具有同等的法律效力。

甲方（盖章）： 乙方（盖章）：

授权代表（签字）： 授权代表（签字）：

日期： 日期：