**合 同 书**

**合同名称： 广东省肇庆监狱2025年网络安全保障服务项目（第二次）采购合同**

**合 同 书**

甲方（需方）： 广东省肇庆监狱 合同编号：

乙方（供方）： 签约地点： 广东省肇庆监狱

根据《中华人民共和国民法典》及竞价文件的承诺，经双方协商，本着平等互利和诚实信用的原则，一致同意签订本合同如下。

**一、合同名称**

合同名称： 广东省肇庆监狱2025年网络安全保障服务项目（第二次）采购合同

二**、合同金额**

本合同金额为 元*。*

合同总价包括了服务期间所有服务费用、设备费用、正常的税金、雇员费用、税费、不可预见费等完成本合同内容所需的一切费用及合同实施过程中应预见和不可预见费用等。乙方不得再向甲方收取任何费用。

**三、合同服务期限**

1.等保测评服务以合同签订之日起60天内完成测评服务，以提交报告给公安并收到回执为准。

2.网络安全加固，网络安全应急响应等服务以2025年8月12日起，服务期限为一年。

**四、合同内容**

**4.1、项目概述**

广东省肇庆监狱拟对已完成定级、备案的第三级信息系统（包括其所含各相关子系统（模块））开展网络安全等级保护测评、整改，网络安全设备升级，安全加固服务，网络安全培训及网络安全应急演练等相关工作。

**4.2、项目范围**

本项目服务范围包括：共计1个已完成定级、备案第三级信息系统（包括其所含各相关子系统（模块））；上述信息系统所涉及的网络、主机、安全设备、应用、数据、机房环境、管理制度等；监狱网络安全设备升级；安全加固服务。具体如下：

（1）信息系统及分布情况：1个第三级信息系统（包括其所含各相关子系统（模块））所涉及的基础软硬件环境等均部署于监狱中心机房。乙方需根据实施阶段对待测信息系统所涵盖的范围进行调整，甲方无需支付额外费用。

（2）网络情况：系统部署与政法内网，政法内网部分包括政法网出口、核心区、安全管理区、生产区（其中生产区包含应用区和数据库区）、存储区等网络区域，通过专线与上级单位互联，进行数据交互。

（3）监狱网络安全设备：天融信应用安全网关系统（IDP特征库、WEB过滤库、专业版快速扫描查杀防病毒库、应用识别特征库1年升级服务许可,适用于NU-31116产品(绑SN)），如果旧版本不能升级，需提供部署新版本。天融信Web应用安全防护系统（WAF产品特征库1年升级License,适用于TWF-52116产品(绑SN)），如果旧版本不能升级，需提供部署新版本。天融信安全管理系统V3(日志服务器系统），原许可型号TAEX\_S，许可类型396e0c65，升级版本，如果旧版本不能升级，需提供部署新版本，系统永久授权。

（4）安全加固服务：对单位终端、操作系统安全加固和优化，对机房网络设备安全加固和优化，包括主机（PC、办公终端）、网络设备和网络设施（交换机、路由器等）打补丁、升级、修补、加固和优化，协助处理应急网络安全事件并提供相关报告，对全狱终端系统、安全设备、网络进行漏洞扫描、修复，要求每月现场驻场处置不少于3个工作日。网络安全加固和优化过程需记录完整技术方法，形成经验教训登记册文档，移交给建设单位。

（5）网络安全应急响应服务：对建设单位网络安全事件进行现场应急处置；节假日提供网络安全检查及运维协助，如线上处理不了则必须当天到达现场处理；合同服务期内组织一次网络安全应急演练，形成网络安全应急演练记录表，记录完整技术方法，移交给建设单位。

（6）网络安全培训：组织一次本地网络安全知识培训，形成网络安全培训记录表，记录完整技术方法，移交给建设单位；提供不少于2人次CISP(或同等国家认证）线下培训课程服务与考试领证服务。

**4.3、项目内容清单**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 序号 | 项目内容 | 内容详情 | 价格 | 备注 |
| 1 | 信息系统等级保护测评服务 | 一个三级系统的等保测评 |  | 一年服务 |
| 2 | 信息系统等级保护整改优化 | 1. 对测评系统进行渗透测试、漏洞扫描并整优化以满足等保要求 2. 对管理制度审核、建设以满足等保要求 3. 对测评系统差距分析、风险评估并整改优化以满足等保要求 |  | 一年服务 |
| 3 | 安全加固服务 | 对全狱终端，服务器，业务系统，安全设备、网络进行漏洞扫描、修复（要求每月现场驻场处置时间不少于3个工作日） |  | 一年服务 |
| 4 | 网络安全设备病毒库，特征库升级服务，审计系统授权数升级服务 | 天融信应用安全网关系统（IDP特征库、WEB过滤库、专业版快速扫描查杀防病毒库、应用识别特征库升级服务许可,适用于NU-31116产品(绑SN)） |  | 一年服务 |
| 5 | 天融信Web应用安全防护系统（WAF产品特征库升级License,适用于TWF-52116产品(绑SN)） |  | 一年服务 |
| 6 | 天融信安全管理系统V3(日志服务器系统），原许可型号TAEX\_S，许可类型396e0c65，升级版本或提供全新版本。 |  | 永久授权 |
| 7 | 网络安全应急响应服务 | 1. 网络安全事件应急处置（现场） 2. 节假日提供网络安全检查及运维协助 3. 组织网络安全应急演练一次 |  | 一年服务 |
| 8 | 网络安全培训 | 1. 组织本地网络安全知识培训一次（具体培训时间由乙方与甲方进行协商确认） 2. 提供不少于2人次CISP(或同等国家认证）线下培训课程服务与考试领证服务 |  | 一年服务 |
| 9 | 合计 |  |  |  |

**4.4、项目目标**

按照《信息安全技术网络安全等级保护基本要求》（GB/T22239-2019）标准要求对第三级信息系统开展等保测评工作，协助监狱完成各类问题的整改及验证工作，合格后出具等级保护测评等相关报告。更新监狱网络安全设备特征库、病毒库，更新日志服务器系统版本或提高全新版本。对监狱终端、服务器、网络设备提供漏洞扫描，修复，提供每月不少于3个工作日的现场驻场服务，协助处理网络安全漏洞及应急网络安全事件。

**4.5、测评标准**

依照我国网络安全等级保护法律法规和制度规范，开展等保测评工作。项目实施过程中应包括不限于以下法规和技术标准：

1.《中华人民共和国网络安全法》

2.《中华人民共和国计算机信息系统安全保护条例》（国务院147 号令）

3.《国家信息化领导小组关于加强信息安全保障工作的意见》（中办发〔2003〕27号）

4.《关于信息安全等级保护工作的实施意见》（公通字〔2004〕66 号）

5.《信息安全等级保护管理办法》（公通字〔2007〕43 号）

6.《关于开展全国重要信息系统安全等级保护定级工作的通知》（公信安〔2007〕861号）

7.《信息安全等级保护备案实施细则》（公信安〔2007〕1360 号）

8.《计算机信息系统安全保护等级划分准则》（GB 17859—1999）

9.《信息安全技术 网络安全等级保护测评要求》（GB/T 28448—2019）

10.《信息安全技术 网络安全等级保护测评过程指南》（GB/T 28449—2018）

11.《信息安全技术 网络安全等级保护基本要求》（GB/T 22239-2019）

12.《信息安全技术 网络安全等级保护定级指南》（GB/T 22240-2020）

**4.6、服务要求**

4.6.1具体要求内容

本项目采购的信息安全评测服务包括差距分析、风险评估、整改建议、等级保护测评和制度审核等，详细如下：

1） 信息系统差距分析活动

信息系统安全等级保护差距分析将根据《信息安全技术 网络安全等级保护测评要求》（GB/T 28448-2019）、《信息安全技术网络安全等级保护测评过程指南》（GB/T 28229-2018）等标准文件的要求，对已定级信息系统，进行系统现状调研，逐项进行合规性检测。其实质是采用基线安全分析的方法，明确当前信息系统与等级保护要求的不符合项及差距。

根据项目的总体要求及信息系统等级保护体系建设现状需要，对信息系统进行差距分析，从安全技术差距分析测评和安全管理差距分析测评两部分进行，对系统各项安全指标进行符合性评估，并标识系统不符合项，明确系统与国家安全等级保护相关标准要求的差距。

2） 信息系统整改咨询服务

信息系统安全建设整改咨询主要是依据差距分析报告，对被测信息系统面临的安全风险进行总结分析，对信息系统不符合信息系统等级保护建设基本要求的部分提供可行性整改建议或方案，从整体上把控内容，主要从技术和管理两方面进行整改，最终能够使被测信息系统在进行安全建设整改后可通过等级保护的测评。

乙方需要根据差距分析中出现的问题、差距分析中存在的差距点、渗透测试发现的信息系统脆弱性以及漏洞扫描结果等相关信息，结合系统实际情况，提供合理、切实可行的整改加固建议，并全程协助各单位进行整改工作，使各系统达到等级保护相应级别的要求。乙方据此完成《网络安全等级保护整改建议书》及其它资料的编撰和整理。

3）信息系统等级保护测评服务

按照等级保护《信息安全技术 网络安全等级保护测评要求》（GB/T 28448-2019）、《信息安全技术 网络安全等级保护基本要求》（GB/T22239-2019）对待测信息系统进行正式的信息安全等级保护测评及复测评，出具公安部门认可的网络安全等级测评报告。

信息系统安全等级测评主要检测和评估信息系统在安全技术、安全管理等方面是否符合已确定的安全等级三级的要求，对于尚未符合要求的信息系统，分析和评估其潜在威胁、薄弱环节以及现有安全防护措施，综合考虑信息系统的重要性和面临的安全威胁等因素，提出相应的整改建议，并根据初次等级保护测评工作中发现的问题进行整改，待整改工作结束后，进行等级保护复测确认，以确保信息系统的安全保护措施符合相应安全等级三级的基本要求，并提交符合国家等级保护测评三级要求的等级保护测评报告。

4） 管理制度审核

本项服务旨在依据国家信息安全管理相关要求，乙方为甲方开展安全建设及整改工作提供咨询指导。乙方依据有关国家标准，审核本项目执行过程中编制的网络安全等保相关制度，并提出修改意见。

5） 协助应检

乙方需配合甲方进行网络安全等保相关检查。具体内容如下：

检查前：需协助对应检系统开展自查，对自查发现的问题进行整改和完善；

检查中：指派专人参与的安全检查，并对检查过程中发现的问题进行记录；

检查后：协助完成网安检查过程中出现的安全问题的整改及编制整改报告。

6） 信息系统风险评估工作

乙方需依据风险评估工作的相关内容，对所有被评估对象进行检查、分析，使其满足项目最终验收要求。须严格按照相关制度和标准的要求，结合被评估单位的具体情况，确定科学严谨的现场实施方案，并完成《风险评估实施方案》的编写。风险评估方案的内容一般包括（但不仅限于）：团队组织：包括评估团队成员、组织结构、角色、责任等内容。工作计划：风险评估各阶段的工作计划，包括工作内容、工作形式、工作成果等内容。时间进度安排：项目实施的时间进度安排。

7）渗透测试

乙方依据已经掌握的安全漏洞信息，模拟黑客的真实攻击方法对系统和网络进行非破坏性质的攻击性测试，并出具《信息系统渗透测试报告》。渗透测试内容应该主要包含外部测试、内部测试，黑盒测试和白盒测试，渗透测试范围应包含第三级系统及各相关子系统，所有的渗透测试行为需在甲方的书面明确授权和监督下进行。

8）漏洞扫描

通过技术手段对第三级系统及各相关子系统进行漏洞扫描，发现可被利用的安全漏洞，并协助项目建设各相关单位进行漏洞修复。进行漏洞扫描后根据扫描结果出具《信息系统漏洞扫描报告》。

9）安全基线核查

基于网络安全法要求以及监管合规要求进行网络安全法责任落实情况预查，为特殊时期的安全提供保障、落实国家政策、法律法规及监管单位的政策合规性的需求。预查内容包括：网络安全保障工作落实情况预查、网络安全信息系统预警及处理方案预查、网络安全管理制度建设与落实情况预查、其他（包含制度、数据、运维、边界、管理、新技术、新应用等）网络安全保护工作情况预查等。基于预查结果出具《信息系统安全配置策略符合性检查报告》、《信息系统安全策略自查报告》、《信息系统安全配置应急自查报告》。

1. 网络加固及现场驻场服务

对单位终端操作系统安全加固和优化，对机房网络设备安全加固和优化，包括主机（PC、办公终端）、网络设备和网络设施（交换机、路由器等）进行打补丁、升级、修补、加固和优化，协助处理应急网络安全事件并提供相关报告，对全狱终端系统，安全设备、网络进行漏洞扫描、修复，要求每月安排工程师现场驻场处置不少于3个工作日。

11）监狱网络安全设备授权服务

天融信应用安全网关系统（IDP特征库、WEB过滤库、专业版快速扫描查杀防病毒库、应用识别特征库1年升级服务许可,适用于NU-31116产品(绑SN)），如果旧版本不能升级，需提供部署新版本。天融信Web应用安全防护系统（WAF产品特征库1年升级License,适用于TWF-52116产品(绑SN)），如果旧版本不能升级，需提供部署新版本。天融信安全管理系统V3(日志服务器系统），原许可型号TAEX\_S，许可类型396e0c65，升级版本，如果旧版本不能升级，需提供部署新版本，系统永久授权。

12）网络安全培训服务

乙方为甲方提供1次本地网络安全培训，形成《网络安全培训会议纪要》。乙方为甲方提供不少于2人次CISP(或同等国家认证）线下培训课程服务与考试领证服务**，**培训费等相关费用由乙方承担。

13）网络安全应急响应服务

乙方需成立项目网络安全应急响应服务团队，团队至少有一名项目经理与一名专职网络安全工程师组成，需提供7\*24技术支持服务，甲方出现网络安全事件需要应急处置时，乙方需30分钟内响应，2小时内安排项目专职工程师到甲方指定现场进行处置，同时节假日提供网络安全检查及运维协助，形成《网络安全事件应急处置统计表》。组织网络安全应急演练一次，形成《网络安全事件应急演练会议纪要》。

14）其他要求

乙方在本项目实施期间应根据本项目实施阶段的国家网络安全等级保护相关要求进行以上工作，因国家网络安全等级保护测评标准变更引起的工作量变更，甲方无需支付额外费用。

4.6.2文档内容

根据以上服务需求内容，乙方负责编制的文档应包括但不限于以下文档内容作为产出物：

（1） 《网络安全设计方案》

（2） 《网络安全等级保护差距分析报告》

（3） 《信息系统风险评估报告》

（4） 《信息系统渗透测试报告》

（5） 《信息系统漏洞扫描报告》

（6） 《网络安全等级保护整改建议书》

（7） 《等级保护测评报告》

（8） 《信息系统安全配置策略符合性检查报告》

（9） 《信息系统安全策略自查报告》

（10） 《信息系统安全配置应急自查报告》

（11）《肇庆监狱2025年网络安全加固技术方案记录表》

（12）《肇庆监狱2025年网络安全应急演练记录表》

（13）《肇庆监狱2025年网络安全培训记录表》

除上述13个中已列明的文档产出物外，乙方应在本项目实施期间根据国家网络安全等级保护相关要求的变化，补充对应的文档产出物，甲方无需支付额外费用。

**4.7、实施要求**

4.7.1实施管理要求

（1）乙方应成立项目管理组织，严格遵守甲方项目管控相关规章制度的要求。在项目实施的各个阶段，按照采购单位相关要求提交文档，并配合其工作。

（2）乙方应基于成熟的项目管理方法论，制订完善的项目管理制度、流程，合理划分项目管理的阶段，借助工程管理工具，在项目实施过程中对项目进行规范化管理，确保项目实施进度和实施质量。

（3）乙方应提供项目管理方案，至少覆盖进度管理、范围管理、风险管理、需求管理、质量管理、资源管理、时间管理、沟通管理等。

（4）乙方应根据项目管理的需要，提供和使用项目管理工具。如甲方要求使用的，必须使用甲方提供的项目管理工具。

（5）乙方提供项目管理工具的，应保证甲方免费使用该管理工具，如涉及版权纠纷，后果由乙方承担。

（6）乙方各阶段产出物采用特殊格式的，乙方需提供相应的打开、编译、运行、修改、打印等工具，并确保甲方无限制的使用；不受版权和知识产权限制，甲方不对工具额外付费。

（7）乙方应认真估算工作量，做好工作量冗余。终验前，乙方须无条件接受并按甲方要求完成各种项目变更，甲方不另行支付费用。

（8）乙方在项目实施过程中所需各种检测工具、项目管理工具等由乙方提供，其结果文档应不依赖于工具而具有可读性，甲方不对此额外付费。

4.7.2.组织人员要求

乙方负责提出项目实施的项目人员配置方案，主要要求如下：

（1）项目实施由乙方安排项目经理配合项目单位，负责项目管理、项目质量控制、项目进度控制、项目测试验收等工作，安排专职工程师配合负责系统测评，系统测试整改，网络安全应急服务等工作。

（2）乙方应提供至少1人担任项目经理**，**要求具有信息系统项目管理师证书，同时具备等保三级及以上项目经验，具有集成、实施项目的丰富经验和较强的沟通协调能力；具有预见和应对项目风险能力。自合同签订之日起至该项目相关系统等保测评全部完成前，项目经理需提供5\*8技术支持服务，进行安全建设咨询与指导工作等。

（3）乙方应提供至少1人专职工程师**，**要求具有信息安全工程师证书（或为CISP注册信息安全专业人员，或为CISAW信息安全保障人员），同时具备等保三级及以上项目经验，具有集成、实施项目的丰富经验和较强的沟通协调能力；自8月12日起，专职工程师需提供7\*24技术支持服务，日常的网络安全应急响应服务，每月不少于3个工作日的现场驻场服务等。

（4）乙方在本项目实施中，应选派工作责任心强、技术水平高、业务熟练、具备等级测评或风险评估实施经验的人员参加本项目的实施。人员总数建议不少于4人，其中测评人员现场不低于2人，且现场人员具有“信息安全等级测评师”或“网络安全等级测评师证书”中级及以上认证证书。

（5）乙方选派的项目组成员应以专职为主，专职人员在项目实施期间不得兼任与本项目无关的其他工作，专职人员比例应不低于 90％。

（6）乙方应在合同签订前提供项目经理与专职工程师名单，同时根据人员要求提供相应的证书或证明文件，在进入系统测评阶段需按要求提供现场测评实施人员名单由甲方确认后，才能进入测评阶段。甲方如认为乙方提供的项目组成员达不到要求，有权要求乙方更换，乙方必须负责在一周之内调换符合甲方要求的项目成员。乙方应按阶段提交项目参与人员名单，经甲方确认。乙方应保证项目组成员的稳定性，如特殊情况需要调整项目组成员的，应提前一个月书面通知甲方，并获得甲方的确认后才能安排调整。

（7）为确保项目顺利实施，项目实施队伍应保持适当的规模，项目组组织结构需分工合理、层次清晰，且分工要为适应项目实施需要。配备人员数量应满足项目需要，原则上每一现场实施人员不得少于1人，不允许职责交叉，不得因为人员离职影响项目的正常开展。

（8）项目经理、专职工程师，测评实施人员应满足项目需要，如果人员不能胜任，甲方有权要求乙方更换人员。乙方原则上不允许更换人员，若更换人员必须书面征得甲方同意，且更换的人员必须具有同等级别和实施经验，并且做好项目交接和资料回收工作；人员搭配应合理，并满足项目实施的要求。

4.7.3.服务质量要求

（1）乙方是本项目技术服务与质量保障的主要承担者和责任人。乙方必须能依据竞价书中各项需求提供及时、高效的技术保障与服务，协助甲方实现系统的长期稳定运行。技术与质量保障的范围包括本项目所涉及的所有服务。在项目规定的技术服务范围及期限内，不得另行收费。具体服务与质量保障要求如下：

（2）乙方方必须拥有完善的技术保障服务体系，能够为甲方提供统一快捷的技术保障服务。乙方必须向甲方免费提供电话、E-mail 技术支撑等方式。

现场实施过程中，在进行渗透检测或其他安全评估时务必做到对生产系统、业务连续性造成任何负面影响的风险实行规避策略。例如系统、应用异常，产生垃圾数据，数据紊乱等。整改过程中，应提供整改需求说明及整改内容，并协助完成整改。

（3）乙方参与项目的所有人员应严格遵守甲方的保密要求签订保密协议或保密承诺书, 并由乙方担保。乙方对于甲方提供的资料，以及本项目实施过程中所涉及的所有文档、数据、介质和相关信息保密，未经许可，不得以任何形式向第三方传播。保密期限不受本项目期限的限制，在本项目履行完毕后，保密信息接受方仍应承担保密义务。如因乙方一方的原因造成泄密，甲方将保留追究其法律责任的权利。

（4）知识转移的目标是乙方采取有效的方式、途径来保证甲方能顺利的接受本项目产生的各项电子版和纸质版文档交付物以及相关项目成果。在采购时，乙方需详细列出知识转移的方案和方式。乙方要规范和完善项目成果、交付物和中间成果的转交过程。乙方在按计划完成和提交项目成果等交付物的同时，这些文档均要以严格的档案管理规范集中组织并保存，提供电子、纸质等多种备查方式，向甲方相关人员开放项目文档，使得甲方可以随时查阅文档，了解和掌握项目中的各种知识。

（5）甲方对项目实施过程中所产生的所有成果（包括相关技术资料、文档等）享有所有权（永久使用权、复制权和修改权等）。除本项目工作所需外，未经甲方书面同意，乙方不得擅自使用、复制甲方的商标、标志、数据信息、文档及其他资料。

（6）乙方应保证在本项目中所有预装和为本项目安装的软件为在中国境内具有合法版权或使用权的正版软件且无质量瑕疵。乙方应保证其所提供的产品及服务不侵犯第三方的知识产权，否则，由此给甲方造成的一切损失由乙方承担。乙方为本项目提供的产品（设备及软件）均为终身授权产品，使用范围为本项目相关系统且无任何限制。

（7）乙方应对项目所涉及的各阶段工作文档的电子版和纸质版，按甲方质量、数量、提供方式、提供时间等要求进行整理，经甲方确认后提交甲方归档。

（8）在项目实施过程的各阶段，本项目相关技术人员适当参与，以工作中的配合关系和传帮带的工作模式进行知识与技能的转移。在此过程中，乙方须将信息安全等级测评和风险评估方法和经验等通过集中培训和文档提交等形式进行转移。

4.7.4.服务期限要求

签订合同后需60天内完成合同规定的三级系统通过网络安全等级保护第三级测评，网络安全加固，网络安全应急响应等服务保障时间为2025年8月12日起，服务期限为一年。在本项目服务期内，必须严格按照合同要求完成相关工作，按时提交各阶段文档，协助完成验收工作。

4.7.5.实施方案要求

乙方必须在项目实施前提交详细的项目实施方案，具体包括技术方案、实施方案、知识转移方案等

**4.8、验收标准**

完成服务需求中所规定的各项内容，保障本项目所涵盖的网络系统全部通过网络安全等级保护第三级测评，完成一年的网络安全应急响应服务。以上工作完成后，按照甲方要求提交①等保测评报告，②过程文档（《网络安全设计方案》、《网络安全等级保护差距分析报告》、《信息系统风险评估报告》、《信息系统渗透测试报告》、 《信息系统漏洞扫描报告》、《网络安全等级保护整改建议书》、 《信息系统安全配置策略符合性检查报告》、 《信息系统安全策略自查报告》、 《信息系统安全配置应急自查报告》），③公安回执，④每月驻场运维人员考勤表，⑤每月网络安全漏洞修复统计表，⑥肇庆监狱2025年网络安全加固技术方案记录表，⑦肇庆监狱2025年网络安全应急演练记录表，⑧肇庆监狱2025年网络安全培训记录表，进行验收。

**五、付款方式**

本项目计划分3 期支付，具体支付方式和时间如下：

5.1首期款：签订合同后 10 个工作日内，乙方书面提出支付申请函及拟支付金额等额的符合甲方财务管理要求的相应发票，甲方确认后启动首期款支付流程，占合同总金额的 30 %。

5.2进度款：合同签订后60天内完成合同规定的三级系统通过网络安全等级保护第三级测评后，乙方书面提出支付申请函及拟支付金额等额的符合甲方财务管理要求的相应发票，甲方确认后启动进度款支付流程，占合同总金额的 30 %。

5.3尾款：合同服务期限到期并通过验收后 10 个工作日内，乙方书面提出支付申请函及拟支付金额等额的符合甲方财务管理要求的相应发票，甲方确认后启动尾款支付流程，占合同总金额的 40 %。

5.4项目合同总价包括了服务期间所有服务费用、设备费用、正常的税金、雇员费用、税费、不可预见费等完成本项目内容所需的一切费用及项目实施过程中应预见和不可预见费用等。乙方不得再向甲方收取任何费用。

**六、违约责任与赔偿损失**

6.1.乙方在合同签订前未按要求提供相应的项目成员名单，视为乙方违约，甲方有权拒签合同，要求乙方支付合同总价10%违约金，并且给甲方造成的经济损失由乙方承担赔偿责任。

6.2.乙方未按合同要求的时间内完成项目清单内容，从逾期之日起每日按本合同总价5‰的数额向甲方支付违约金，期10天以上（含10天）的，甲方有权终止合同，要求乙方支付合同总价10%违约金，并且给甲方造成的经济损失由乙方承担赔偿责任。

6.3.合同期内甲方和乙方双方无正当理由终止合同的，违约方须向守约方支付合同总额 20%的违约金。如因乙方违约导致合同解除的，乙方应返还甲方已支付的全部合同款项。违约金不足以弥补守约方所受损失的，守约方有权进一步追偿。若甲方解除合同后，乙方须在接到甲方解约通知之日起 10 天内退回甲方已支付合同价款。

6.4合同期内，如乙方出现2次或以上未按合同要求或时间完成服务的，视为乙方严重违约，甲方要求立即解除本合同，乙方应返还甲方已支付的全部款项，且甲方有权要求乙方按合同总额20%支付违约金。

**七、争议解决方式**

本合同发生争议，由双方协商或由政府采购监督管理部门调解解决，协商或调解不成时向有管辖权的人民法院提起诉讼。（本合同的诉讼管辖地为肇庆有管辖权的法院）（在诉讼期间，除有争议部分的事项外，合同其他部分仍应继续履行）。

**八、不可抗力**

任何一方由于不可抗力原因不能履行合同时，应在不可抗力事件结束后1日内向对方通报，以减轻可能给对方造成的损失，在取得有关机构的不可抗力证明或双方谅解确认后，允许延期履行或修订合同，并根据情况可部分或全部免于承担违约责任。

**九、保密**

9.1乙方必须采取措施对本合同实施过程中的技术资料保密，否则，由于乙方过错导致的上述资料泄密的，乙方必须承担一切责任。合同内容完成后，甲、乙双方均有责任对本合同的技术保密承担责任。

9.2未经甲方事先书面同意，乙方不得将由甲方为本合同提供的技术资料提供给与本合同无关的任何第三方，不得将其用于履行本合同之外的其它用途。即使向与履行本合同有关的人员提供，也应注意保密并限于履行合同所必需的范围。

9.3如果甲方有要求，乙方在完成合同后应将有关资料还给甲方。

甲方（盖章）： 乙方（盖章）：

地址： 地址：

法定代表人/负责人： 法定代表人/负责人：

委托代理人： 委托代理人：

电话： 电话：

开户银行： 开户银行：

账号： 账号：

签约时间： 年 月 日 签约时间： 年 月 日