**ETC发行服务系统2025年度硬件和支撑**

**系统技术保障服务项目**

**合同主要条款**

**（本合同主要条款供双方签订合同参考，采购人可根据项目的实际情况增加条款和内容）**

甲方（采购人）：

乙方（成交供应商）：

**一、项目内容：**

**二、服务地点、时间、人员**

2.1乙方为甲方提供的服务期限为 2025 年 7 月 1 日到 202 6年 6 月 30 日（具体以项目实施日期为准）

2.2服务地点： 陕西省西安市以及ETC发行服务网点 （根据项目的实际情况确定）

2.3服务人员要求：人员配置要求必须满足服务要求。

**三、权利和义务**

3.1甲方的权利和义务

3.1.1甲方有权指派专门人员或者单位对乙方的工作进行全程监督管理；

3.1.2甲方应按合同约定向乙方支付服务费用。如乙方服务未达到合同要求，甲方有权拒付未达到要求部分的款项；

3.1.3甲方有权要求乙方提供与相关服务内容有关的相关信息；

3.1.4甲方有权得到符合合同要求的所有服务；

3.1.5乙方完成所有协议约定内容后，甲方根据项目实施情况出具的客观公正的书面用户验收意见。

3.2乙方的权利和义务

3.2.1合作过程中乙方应指派专门的业务负责人负责合作事项的全程沟通及协调工作；

3.2.2乙方应遵守甲方有关合作事项的各项管理规定，及时报告工作进度，在规定时间内完成相应工作；

3.2.3甲方在工作质量、工作进度、工作内容等方面提出意见及建议，乙方应及时响应并有效改进；

3.2.4不得转包、分包；

**四、支付方式**

4.1合同签订生效并进入服务期后15日内，供应商按付款要求开具合同发票，采购人支付合同价款的 65%（服务商须提供同等金额的银行保函）；合同剩余价款的35%，在每月提交相应维护报告后 15 日内支付当月的服务费；最后 1 个月的服务费，在服务期满并验收合格后 15 日内进行支付。

**五、违约责任**

5.1按《中华人民共和国民法典》中的相关条款执行。

5.2未按合同要求提供服务或服务质量不能满足技术要求的，甲方有权终止合同。对擅自开展合同内涉及的系统软件开展功能修改调整、版本升级等操作，每次扣除维护服务费2000元。若系统调整后影响全省业务正常运行达到6小时的，每次扣款5000元；每增加6小时，增加5000元，24小时内最高扣款金额20000元。影响全省业务正常运行超过24小时的，根据造成的实际损失及影响进行责任追究等。

5.3因乙方违约造成甲方损失的， 由乙方承担全部的损失赔偿责任，包括但不限于直接经济损失及甲方因此开支的交通费、公证费、鉴定费、诉讼费、仲裁费、律师费、保全费、保险费等一切费用。

**六、保密要求**

项目实施过程中所收集、产生的所有与本项目相关的文档、资料，包括文字、 图片、表格、数字等各种形式所属权均归属甲方。服务商必须对所涉及到的内容保密，服务商及服务人员应按照要求签署《保密协议》。（见附件）

**七、网络安全要求。**

服务商具备健全的网络安全服务体系，具有网络安全隐患排查、完善加固、预警监测、应对攻击等服务能力，配备具有相关技术能力的网络安全专职人员，为本项目提供漏洞检测、策略配置、加固整改、安全监测、应急处置等保障措施，确保系统安全稳定运行。服务商未发生过重大网络安全事件，按照中心项目的统一要求签署《网络安全责任协议》。（见附件）

**八、合同争议的解决**

8.1合同一经签订，不得擅自变更、中止或者终止合同。对确需变更、调整或者中止、终止合同的，应按规定履行相应的手续。

8.2采购人在合同的履行期间以及履行期后，可以随时检查项目的执行情况，对招标标准、招标采购内容进行调查核实，并对发现的问题进行处理。

8.3合同争议的解决：合同在履行过程中发生的争议，当事人双方应协商解决，协商达不成一致时，可向合同履行地人民法院提起诉讼。

**九、合同生效及其他**

9.1本合同经甲乙双方签字盖章后生效；

9.2本合同中所带的附件，具备合同本身同样的法律效力；

9.3本合同一式 份，其中，甲方 份，乙方 份。均具有同等法律效力。

9.4乙方收款账号信息如下：

9.4.1开户名称： ；

9.4.2账 号： ；

9.4.3开户银行： ；

9.5本合同未尽事宜，双方以补充合同完善。

甲方：（盖章） 乙方：（盖章）

法定代表人/授权代表： 法定代表人/授权代表：

地 址： 地 址：

开户银行： 开户银行：

账 号： 账 号：

电 话： 电 话：

传 真： 传 真：

签订日期： 年 月 日 签订日期： 年 月 日

附件：

**保 密 协 议**

甲方与乙方签订《\*\*\*\*\*\*合同》。为了在项目实施的过程中，使甲乙双方的保密信息、知识产权和相关的合同信息不受到侵害。为此甲、乙双方在履行本协议时，均应遵守《中华人民共和国保守国家秘密法》和《反不正当竞争法》等法律规定，并严格按照以下条款规定开展工作：

**一、保密内容**

（一）乙方需要保密内容：乙方在履行合同的过程中所获悉的甲方提供的系统信息资产台账、系统网络拓扑信息、系统配置信息、系统运行的数据等，以及经甲方声明需要保密信息。

（二）甲方需要保密内容：乙方在系统运维服务中使用的流程、方法以及乙方声明需要保密的其他信息。

**二、保密信息的使用**

（一）甲方应指定专门的项目协调人员配合乙方工作，乙方在履行合同过程中如需了解或获取甲方相关资料或信息，应向甲方项目协调人员索取。

（二）甲方项目协调人员应做好保密信息管理及调研情况的记录工作，乙方应予以配合。

（三）乙方可按以下方式获取信息:书面、交付项目、启动信息存取（如存在数据库中的信息）。

**三、保密的范围**

（一）乙方只在本项目需要时才能使用甲方提供的秘密信息。乙方应将甲方提供信息的使用限制在与本项目有关的人员、保密协议签署者范围内。

（二）甲方应将乙方在本项目中使用到的流程和方法等技术信息限制在与本项目有关的人员、保密协议签署者范围内。

**四、保密义务**

（一）未经许可不得获取对方与本次工作无关的秘密信息；

（二）不得向任何第三方披露、转让或协助使用上述秘密信息；

（三）如发现上述秘密被泄露或者自己过失泄露，应当采取有效措施防止泄密进一步扩大，并及时向对方报告；

（四）凡未经对方书面同意，一方以直接、间接、书面、口头等形式为第三方提供第一条保密内容的行为均属违反保密义务的行为。但以下情况不属于违反保密义务：

1.获取或披露一方已公开发表，或已为公众所知的信息；

2.获取或披露一方已书面授权公开的信息；

3.获取的信息属于一方通过合法手段从第三方在未受到任何限制的情况下获得的；

4.根据法律、法规，司法或行政命令的要求向有关国家机关提供他方的秘密信息，提供前必须经过双方的书面认可。

**五、保密期限**

甲、乙双方确认，双方的保密义务从本协议签署之日起生效。自本合同生效之日起算，保密期限为无限期。

**六、违约责任**

（一）如果一方不履行本协议第四条所规定的保密义务，应当承担给对方造成的直接损失的赔偿责任，并承担合同金额20%的违约金。

（二）因一方的违约行为侵犯了另一方的合法权益，对方可以选择根据本协议要求其承担违约责任，或者根据国家有关法律、法规要求其承担侵权责任。

（三）任何一方及其工作人员未按照本协议约定使用保密信息或者泄露保密信息而触犯有关法律，一方都可以有权按照本条的规定取得赔偿，还将依法追究另一方的行政及刑事责任。

**七、争议的解决**

甲乙双方友好协商解决本协议中的争议。协商不成的，任何一方都有权向甲方所在地人民法院即西安市未央区人民法院提起诉讼。

八、法律适用、协议文本及效力和变更

（一）本协议适用中华人民共和国的法律。

（二）本协议的任何修改必须经过双方协商一致，并以书面方式确认方为有效。

（三）本协议经双方法定代表人、负责人或授权代表签字并加盖单位公章后生效。

附件：

**网络安全责任协议**

陕西省高速公路收费中心（以下简称“ 甲方 ”）委托 （以下简称“乙方”）进行运维服务，为加强信息系统网络安全管理工作，保障系统安全稳定运行，按照《中华人民共和国网络安全法》规定，网络安全等级保护及部、省网络安全有关要求，结合《陕西省高速公路收费中心信息系统网络安全管理办法》，经甲乙双方友好协商，签订本网络安全责任协议：

**第一条 术语定义**

1.本协议甲方关键岗位为系统管理员、安全管理员、审计管理员。

2.本协议乙方关键岗位为参与系统设计、开发、测试、运维等系统全生命周期的所有相关人员。

**第二条 总体要求**

双方要贯彻落实网络安全法律法规，认真执行交通运输部、省委省政府、省交通运输厅和甲方的网络安全规章制度，

落实网络安全责任，把网络安全工作纳入重要工作，明确网络安全关键岗位人员及职责，开展关键岗位人员背景审查，与关键岗位人员签订网络安全责任书 和保密协议，共同保障系统安全稳定运行。

**第三条 建设要求**

1.新建、升级改造的系统，乙方提供的硬件、软件和服务，要符合国家法律、行政法规的规定以及强制性国家标准要求，并通过权威机构的安全认证。

2.新建、升级改造的系统或现有系统新增功能上线前，乙方要委托具有网络安全相关专业能力的机构进行安全检测，安全检测要至少包括系统部署环境评估、安全漏洞扫描、基线配置核查、渗透测试、代码安全审计五方面内容，出具安全检测报告，向甲方报送安全检测报告并提供系统资产清单（所有运行需要使用的软件、插件、进程、IP、端口等）后，系统或新增功能方可正式上线。

3.乙方要严格按照软件工程规范、系统安全需求进行业务应用系统设计开发， 不得在程序代码中植入后门、隐蔽信道和恶意代码，同时要关闭高危端口，与业务无关的端口、进程和服务。

**第四条 服务要求**

1.乙方要制定完善网络安全服务规范，建立更新系统资产台账，形成系统网络拓扑图，清理已被替换的老旧系统、未关停的测试系统、废弃无用系统等“僵尸系统 ”，确保资产信息全面准确。

2.乙方要定期开展系统网络安全意识教育和专业技能培训，提升工作人员网络安全意识和技能，从事甲方安全服务人员要具备漏洞检测、策略配置、加固整改、安全监测等技术能力，能够熟练使用网络安全常见产品和工具。

3.乙方要定期开展漏洞扫描、配置核查、渗透测试等系统自查行动，建立漏洞隐患清单，彻底消除口令问题，严格密码存储管理要求，确保中高危隐患清零。

4.乙方要保存系统基础配置信息，留存的系统相关日志不少于六个月，并定期对日志进行审计分析，严格控制运维工具使用，规范日常运维操作行为，形成运维过程相应表单记录。

5.乙方要及时清理离职离岗人员权限，按照最小化原则进行账号授权，及时升级安装最新补丁和杀毒软件，确保系统软件升至最新版本。

6.乙方要加强系统介质管理，严格介质使用要求，杜绝专网设备违规外联，严格边界访问控制，定期核查优化安全策略。

7.乙方要严格落实国家和行业对数据和个人信息保护相关要求，建立数据访问管理清单，做好数据备份存储工作，定期检查数据有效性，采取脱敏处理及存储加密等安全措施，确保个人信息安全。

8.乙方要加强系统安全风险预警响应，积极利用已有监测方式、第三方监测手段或自行开发的脚本，做好系统异常行为监测，及时处置告警信息，确保系统正常运行。

**第五条 责任追究**

若乙方未落实本网络安全责任协议内容或因防护不当、未及时发现攻击行为， 造成部、省、公安、网信等有关部门通报，发现并通报1次，扣除服务费5000元；造成网络安全事件时，将按照国家，部、省、甲方等网络安全相关规定，根据造成的实际损失、影响，上报有关部门，同时进行责任追究。

**第六条 争议解决**

双方友好协商解决本协议中的争议。协商不成的，任何一方都有权向甲方所在地人民法院提起诉讼。

**第七条 法律适用、协议文本及效力和变更**

1.本协议适用中华人民共和国的法律。

2.本协议未尽事宜按国家有关法律法规、行业和甲方有关规定执行。

3.本协议的任何修改必须经过双方协商一致，并以书面方式确认方为有效。

4.本协议经双方法定代表人、负责人或授权代表签字并加盖单位公章后生效。