采购项目编号：ZMZB2025YYXY-201

西安音乐学院

2025年网络安全运维服务项目

（合同书）

甲方：西安音乐学院

乙方：西安云唐电子科技有限公司

2025年9月

合同书

甲方：西安音乐学院

乙方：西安云唐电子科技有限公司

依据《中华人民共和国民法典》《中华人民共和国政府采购法》及其他有关法律法规的规定和本项目竞争性磋商文件的要求及磋商结果，遵循平等、自愿、公平和诚信的原则，双方就西安音乐学院 2025 年网络安全运维服务项目相关事项达成一致意见，订立本合同。

一、该项目涉及的合同文件及解释顺序

1、本合同协议书；

2、成交通知书；

3、竞争性磋商文件、磋商响应文件；

本合同签订后，双方依法签订的补充协议、备忘录也是本合同文件的组成部分。

二、合同标的

（一）项目名称：西安音乐学院 2025 年网络安全运维服务项目

（二）项目地点：西安音乐学院

（三）服务期限： 2025 年 10 月 23 日 至 2026 年 10 月 22 日

奇安信网站云防护安域授权期限：2025 年 10 月 23 日至 2026 年 10 月 22 日

（四）服务的主要内容及清单：

1. 资产梳理和治理服务

每半年通过非凡资产安全运维服务平台 OKSOP 系统，对全校提供服务的信息资产进行全面梳理，包括资产管理信息、系统信息、网络信息等，确定资产范围，形成信息资产梳理清单。

每半年通过奇安信网站云防护安域系统，对全校的 WEB 资产进行梳理，发现全校 WEB 资产及 Webshell 后门、网站暗链接、敏感内容、僵尸网站等情况，形成 WEB 资产治理清单。

2. 安全评估服务

通过非凡资产安全运维服务平台 OKSOP 系统，每季度对学校信息资产存在的脆弱性进行分析，参考相关的国际标准、国内标准和教育行业的相关规范，满足《网络安全法》《信息安全技术信息系统风险评估规范（GB/T 20984）》《信息安全评估指南》等相关标准和要求，通过漏洞扫描、安全配置核查、渗透测试等技术手段和管理措施，在物理安全、网络安全、主机安全、应用安全、数据安全、安全管理机构、安全管理制度、人员安全管理、

安全运维管理、安全建设管理等方面实施安全评估服务，并通过安全专家风险分析，清晰展现信息资产面临的风险，输出《第 X 季度安全评估报告》。对存在中高危安全隐患的信息资产，输出《XX 整改报告》，包括所发现的安全问题和解决方案，用于相关责任部门进行整改。

根据西安音乐学院信息系统建设情况，对新上线信息系统及网站等资产实施上线前安全评估和复检，输出《XX 上线前安全检测评估报告》，用于相关部门进行整改，确保信息系统上线前的安全稳定运行。

3. 安全加固服务

部署非凡资产安全运维服务平台 OKSOP 系统，针对西安音乐学院安全评估发现的各类安全风险和权威机构发布的重大安全漏洞、危险和预警，从管理和技术等角度制定有针对性的整改和加固方案；对存在中、高风险级别以上的信息资产，协助实施安全加固，提高信息资产安全级别，最大程度的避免、降低各类安全事件的出现，保障信息资产的安全、稳定运行。安全加固服务结束后输出《XX 安全加固报告》，并进行安全漏洞的相关复测。

4. 安全应急与保障服务

在西安音乐学院发生各类网络安全事件时，第一时间提供应急响应和处置服务，按照安全应急响应预案，及时采取有效的应对措施，控制安全事件造成的影响范围，缩小损失，排查问题来源，恢复信息资产正常运行，应急响应结束后，输出《XX 应急响应报告》。

每半年开展一次网络安全应急演练，提高相关人员网络安全防护意识，增强网络安全预测、防御能力，强化应急响应和处置等方面的能力。

按照学校要求和上级部门要求，在寒暑假、节假日、敏感时期、网络安全攻防演习、监督检查、专项排查等重要期间提供安全保障服务，制定安全保障方案，确保在此期间信息资产安全稳定运行。当出现安全事件时，提供安全应急响应服务。保障服务结束后，输出《XX 保障服务报告》。

5. 安全咨询与培训服务

通过安全评估等工作的实施，全面了解校园网络安全现状，分析存在的安全风险，协助规划设计网络安全防护体系，构建全面安全的管理体系，提升网络安全风险管控能力。面向网络安全管理员提供每年 1 次的安全培训，包括个人安全防护意识和措施、安全攻防技术等培训内容；每年开展 1 次校级网络安全攻防演习。

6. 安全运维驻场服务

提供 2 名网络安全专职人员驻场，负责梳理和完善网络信息安全管理制度、管理流程；

安全设备日常管理、运维；网站、信息系统等资产的安全运维；安全日志汇总分析，安全隐患排查及处置、安全事件监控及处置；以及其他网络信息安全相关工作。

1.驻场人员资质要求

大专学历，计算机或通信工程相关专业，网络与信息安全专业，具有 CISP 证书，2 年以上网络安全工作经验。

2.驻场人员技能要求

熟悉计算机及网络安全技术，熟练掌握相关网络设备、安全设备、操作系统、数据库的配置管理及安全加固；熟悉信息安全技术模型中涉及通信网络信息防泄漏、风险评估、渗透测试的相关知识；熟悉主流国产网络安全设备的配置与运维管理；具有良好的文档能力和问题处理经验；具有良好的沟通能力、团队合作精神和服务意识；有较强的责任感，可以独立自主完成任务；遵纪守法，无犯罪记录。

3.考核要求

驻场人员须严格遵守西安音乐学院的各项管理规定。服务期内未经学校同意不得随意更换驻场人员，驻场人员的技术能力若不满足学校要求的，乙方必须无条件立即更换，每更换一名技术人员，服务期顺延 30 天；如乙方驻场人员变动两次（含）以上，出现一次甲方扣除成交价的 10%；乙方未按时按量按质提供服务，甲方拒付所有服务费用；如因乙方驻场人员造成学校网络安全事件（事故）发生，乙方需承担相应责任。

7.人员配备及岗位职责

序号	人员	学历	工作年限	岗位职责
1	袁毅	大专	23 年	项目经理
2	龚彬彬	大专	18 年	技术负责人
3	王特	大专	3 年	安全专家
4	段若琳	大专	4 年	驻场人员
5	李小健	大专	18 年	驻场人员

8.云安全服务要求

通过部署奇安信网站云防护安域系统，为学校提供如下云安全服务内容：

序号	指标项	功能要求
1	产品形态	支持云端防护账号交付，以 SaaS 的方式为学校提供网站安全防护服务。

2	性能规格	配置 60 个域名的网站安全云防护。包括 Web 攻击防护、网站缓存加速、≥10Gbps 的 DDoS 攻击共享型防护、≥30Gbps 高防 DNS、≥2 千 QPS 正常业务请求并发；提供≥6TB 正常业务流量、≥10GB 的 Web 访问日志下载流量、60 个非标准端口。提供 1 年防护服务：产品远程技术要求（包含防护接入、防护过程中产品问题支持），7x24 小时电话支持，以及防护周期内的防护引擎、防护规则免费升级。
3	IPv4/IPv6 双栈	支持 IPv4/IPv6 双栈网站防护服务。
4	WEB 攻击防护	支持服务器隐身功能，使得黑客无法获取服务器真实 IP 地址，防止黑客对服务器的各种攻击。
		支持能识别和阻断 SQL 注入攻击、Cookie 注入攻击、命令注入、跨站脚本攻击、文件包含攻击、LDAP 注入、XPATH 注入、爬虫攻击、Struts2 命令执行攻击等常见的 WEB 攻击，防止网站敏感信息泄露。
		支持细粒度的 WEB 防护配置，可以对不同 Web 安全漏洞类型设置白名单，当设置生效后。
		支持自定义防护页面功能，即当检测到定义的响应码时可以跳转到指定 URL。
		支持用户自定义 URL 弱口令检测防护，对检测参数和口令复杂度进行配置。
		支持自定义防护特征，针对 HTTP 请求方法、参数、头部等配置自定义防护规则。
		支持开启监听模式，只检测不拦截攻击请求，并记录攻击日志。
5	DDoS 攻击防护	支持对 SYN Flood 攻击、Frag Flood 攻击、ACK Flood 攻击、UDP Flood 攻击、ICMP Flood 攻击等常见的流量型 DDOS 攻击进行清洗。
6	CC 攻击防护	支持强制缓存功能，当触发 CC 攻击防护时，可对用户自定义配置的 URL 按照选定的类型进行缓存，如样式、JS、图片、静态 HTML、首页、多媒体文件、文档类型、压缩文件等，保证相关内容仍可正常对外访问。
		支持根据源站总并发连接数和访问源单 IP 并发连接数对攻击进行 CC 判断，并发连接数超出管理员配置并发连接数阈值后，对攻击源进行自动防御、JS 防御或图片验证防御。
7	高防 DNS	支持智能 DNS 解析；网站 NS 方式接入，即由防护平台提供 DNS 域名解析，提供记录解析、AAAA 记录解析、CNAME 记录解析等 DNS 解析方式。
		支持针对 DNS 的攻击防护，如 DNS Query Flood 攻击、DNS replay food 攻击等流量型攻击。
8	爬虫攻击防护	支持对客户端环境和信息进行深度分析和识别，拒绝来自非正常环境的访问。
		支持基于 IP、URL、Cookie 名称、Header 名称等参数进行访问频率限制。
9	敏感词过滤	内置完备的敏感词信息库，开启默认防护策略时，可主动监测网站首页有无敏感词，如果存在便产生告警。

		支持用户自定义 URL、敏感词内容，细粒度的对响应方向进行检测，当响应内容包含自定义敏感信息时，则可对内容进行告警、替换*、阻断和重定向动作。
10	访问控制	支持对在特定时间段内某 IP 地址或 IP 地址段是否能够访问特定 URL 进行访问控制。
		支持对不同国家和中国的不同省市能否访问保护网站进行访问控制，并能够基于 IP 地址添加例外访问黑白名单。
		支持对包含特定的 USER-Agent 字段内容的访问进行访问控制。
11	CDN 加速缓存	有全国性的缓存节点机房，按照最小响应时间，最优访问服务等智能缓存算法为用户自动选择缓存节点机房，以提升用户访问效果。
		支持对 CSS、JS、图片、静态 HTML、首页、多媒体文件、文档类型、压缩文件等类型进行缓存。
		支持对单个 URL 或者全站进行手工缓存刷新控制的功能。
		支持 URL 缓存黑白名单功能，可以对特定 URL 进行是否缓存进行控制。
		支持浏览器缓存加速功能，即将待访问的内容缓存在访问者浏览器上，用户无需请求服务器即可完成对网站页面文件的访问。
12	日志报表	支持 WEB 攻击报表，包括 WEB 攻击次数，攻击 IP 数，攻击者全国分布图，攻击 IP TopN。
		WEB 攻击日志包含攻击类型、攻击 IP、IP 归属地、攻击 URL 及参数，攻击次数等参数。
		CC 攻击报表包括 CC 攻击次数，攻击 IP 数，攻击者全国分布图显示，攻击 IP TopN。
		CC 攻击日志包含攻击类型、攻击 IP、IP 归属地、攻击 URL、攻击事件、攻击次数等参数。
13	安全报表	支持自定义时间段的报表功能，能直观的显示本周及历史周网站遭受的 WEB 攻击、CC 攻击等攻击情况。
		支持月度简报功能，能每月定时向指定邮箱发送月度简报，展示网站安全防护情况。
		报表内容包括拦截漏洞数、本周遭受的 CC 攻击数、攻击次数最多的 IP、受攻击最多的域名，WEB 攻击的趋势报表、遭受的 CC 攻击的趋势报表，WEB 攻击方式 TopN、遭受 CC 攻击的 URL TopN，WEB 攻击源 IP 全国分布位置，CC 攻击源全国分布位置等内容，安全要求 PDF、CSV 格式导出下载。
14	攻击告警	支持对 Web 攻击、CC 攻击、爬虫攻击进行自定义攻击阈值告警。同时要求自定义统计周期、告警方式（邮件、短信）、告警接收人、告警接收组信息。要求将多个告警人添加为一个告警组，要求对同一告警组下所有告警人做相同告警配置。
15	一键关站	支持一键关闭外部对源站的访问，达到一键关站的效果，并可以指定关站响应码或者制定响应页面。
16	多因子认证	支持登录账号的多因子认证，包含：密码、验证码、短信验证方式，确保登录安全。

17	三元用户管理	支持超级管理员、普通管理员、审计管理员等管理员角色。超级管理员可以创建其他所有管理员并拥有系统最高权限；普通注册管理员只可以查看并配置自己域名的权限；审计管理员智能审计配置及日志报表。
18	移动运维	支持安卓/IOS 版手机 APP 运维客户端，可要求手机接入防护、一键关站（一键处置）、一键回源、WEB 防火墙开启/关闭、缓存开关设置、账号管理等功能。
19	API 安全	针对网站中 API 接口提供细粒度梳理与精细化防护，包括 API 资产自动识别、API 业务统计、API 安全防护等功能。
20	防篡改	管理员可以通过调整配置将被保护的网站静态资源主动爬取缓存到 WEB 安全云防护系统的缓存服务器中。当源站出现网站服务停止、网站服务器宕机、网络异常等情况无法正常提供服务时，WEB 应用安全云防护系统可以使用缓存的静态页面文件继续对外展示网站页面，保证在重要时期网站持续对外提供正常服务。
21	数据安全	支持对网站中展示的个人信息、图片属性中的敏感信息、文件属性中的敏感信息进行防护，对特定页面和下载文件加水印，防止业务数据泄露，并可进行敏感数据溯源。
22	端口分离	端口分离开启后可使用指定的端口作为访问端口，为客户节省大量 IP 地址资源。
23	服务资质	网站云防护服务厂商奇安信具备如下资质： CCRC 信息安全服务资质-应急处理（一级，为最高级）证书； ITSS 云计算服务能力标准符合性证书(SaaS 服务(二级及以上，一级为最高级)； CNCERT 应急服务支撑单位(APT 监测分析)资质证书； CNNVD 技术支撑单位（一级，为最高级）资质证书。

9. 培训、授权要求

（一）培训要求

为确保项目实施完成后，各应用系统和业务系统能够顺利投入运行，乙方需加强对项目管理人员、系统使用人员、技术保障人员的全面安全学习培训工作。通过相关培训，要达到以下目标：

1. 使项目相关人员能够正确认识理解本次安全建设项目重点意义；

2. 系统使用人员能够熟练掌握安全系统常用功能、操作方法、工作流程；

3. 使学校的相关技术人员，如系统管理员、运维管理员等能够具备系统安全管理、安全运维等能力；

4. 技术保障人员能够全面的了解安全系统基本原理、技术特性、操作规范、运行规范和管理维护，能独立对设备/系统进行管理、运行、故障处理及日常测试维护等工作，确保系统能正常运行；

5. 使安全管理相关人员了解用户信息系统的安全体系的框架及具体内容；

6. 提高本项目相关工作人员的信息安全意识。

（二）授权要求

要求在 2025 年 10 月 22 日前完成云安全服务授权。

三、合同总价和结算方式

（一）合同总价（小写）：￥380000.00 元（大写：人民币叁拾捌万元整），合同总价为固定总价，一次包死，不受市场价变化或实际工作量变化的影响，合同总价为含税价，乙方提供服务、产品所发生的包括但不限于一切税（包括增值税）费、人工费、交通费等所有费用都已包含于合同总价款中。如因乙方漏报、误报等导致的费用差异均由乙方自行承担。

（二）支付方式：银行转账

名　　称：西安云唐电子科技有限公司

开 户 行：中国民生银行股份有限公司西安分行营业部

账　　号：161273248

甲方付款前，乙方应开具等额的增值税普通发票并配合甲方办理相应付款手续。否则，甲方不承担逾期付款的责任。

（三）货币单位：人民币；

（四）结算方式：

甲方按照进度支付费用：（1）项目中期验收合格后，甲方向乙方支付合同总额的 50%，即￥190000.00 元，（大写：人民币壹拾玖万元整）；（2）项目完成并验收合格（甲方以出具书面验收合格文件的形式予以确认）后支付合同总额的 50%，即￥190000.00 元，（大写：人民币壹拾玖万元整。）

四、验收

（一）验收：乙方完成服务内容后，向甲方提出验收书面申请，甲方接到乙方验收申请后组织验收（必要时可聘请相应专家或委托相应部门验收，由此而产生的所有费用均由乙方承担），验收合格后，出具书面验收合格证明文件。

（二）验收结果作为付款依据，乙方需要向甲方提交实施过程中的所有资料，以便甲方日后管理和维护。

（三）验收依据：合同文本、合同附件、竞争性谈判文件、乙方的响应文件以及国内相应的标准、规范。

五、双方承诺

（一）甲方责任：

1. 甲方负责提供项目相关详细资料；

2. 甲方按照合同约定向乙方支付服务款项；

3. 甲方提供服务过程中相关联系人信息，以保障服务项目的顺利实施；

4. 在服务期内，甲方可通过电话方式向乙方技术人员咨询有关技术问题，远程不能解决的，1 小时内到达现场协助解决。

（二）乙方责任：

1.为了保障本次服务项目高质量地完成，乙方按照项目管理的要求和方法对本项目进行科学的管理。乙方选派专业的服务人员以勤勉尽责的态度履行本合同中约定的服务工作。

2.乙方应严格按照本合同约定的进度及响应时间按时提供服务。服务进度延误的，乙方应按照本合同的约定承担逾期责任。

3.乙方在甲方提供的场所实施服务的过程中，应严格遵守甲方和乙方的管理要求，包括安保、环保、消防、卫生、网络管理、保密等方面要求，防止发生人身伤亡和设备事故。因乙方服务人员的过失导致甲方发生人身或财产损失的，乙方应当予以赔偿。乙方实施服务的过程中发生设备、人身、交通、火灾等事故由乙方承担全部责任及费用，甲方不承担任何责任。

4. 乙方自备完成服务所需要的软、硬件工具。如果甲方提供了服务工具，乙方应当妥善使用，在使用完毕后完好归还工具。若因乙方行为导致甲方所提供服务工具损坏、灭失的，乙方应照市价赔偿。

六、保密

（一）乙方有责任对获知的甲方技术或商业秘密保守机密、数据、资料等非公开信息，并对系统中涉及甲方业务的资料、数据保守机密。

（二）乙方承诺，未经甲方书面同意，乙方不得将涉及本项目所有的直接或间接数据、信息、密码等资料内容向第三方透露、公开，否则，乙方应按照该合同总价的 30%向甲方支付违约金。若该违约金无法弥补甲方损失（包括间接损失、直接损失），甲方有权向乙方进行追偿。

七、知识产权

（一）乙方应保证产品及服务不会出现因第三方提出侵犯其专利权、商标权、著作权或其它知识产权而引发法律或经济纠纷，否则由乙方承担全部责任。任何被乙方用于未经

授权的行为所造成的违约或侵权责任由乙方承但。甲方在代替乙方承担相应责任后，有权就全部损失（包括但不限于直接损失及代替履行责任和追偿而产生的全部律师费、诉讼费、保全费、公证费、交通费等间接损失）向乙方追偿。

（二）本合同项下服务过程中所涉及软硬件的知识产权属于乙方，甲方对其享有使用权。

八、不可抗力

（一）本合同签订的任何一方因战争、火灾、水灾、台风、地震等不可抗力事件导致无法履行其合同义务时，除下述规定外，经甲方书面同意后，本合同执行时程将延长与上述不可抗力持续时间相等之日数。

（二）因不可抗力致使无法履行义务一方应立即书面通知对方，并于不可抗力发生后3天内，将当地主管机构出具的证明文件邮寄给对方。

（三）如不可抗力影响合同履行超过10天，双方应就合同的进一步履行与否进行磋商。

九、违约责任

依据《中华人民共和国民法典》等的相关条款和本合同约定，乙方未全面履行合同义务或者发生违约，甲方有权终止合同，依法向乙方进行经济索赔。

（一）除本合同第七条规定的不可抗力之外，因乙方原因造成乙方没有按时、保质地完成安全服务，乙方应向甲方支付违约金（合同总价的0.5%/周），直至合同解除。若累计延迟超过30天，甲方有权单方解除合同，若无法弥补给甲方造成的损失，甲方有权向乙方追偿。

（二）合同履行过程中，甲方有权对乙方提供的服务进行检查和监督。如甲方发现不合理之处或乙方未按照合同的要求配置工作人员、完成服务，在沟通无效的情况下，甲方有权向乙方下达整改通知书，并要求乙方限期整改。乙方在接到甲方的通知后，应按照甲方的要求积极做出相应改正。

如乙方接到甲方通知后不予答复或在约定时间内，不能予以改正或甲方向乙方发出限期整改通知书总计超过3次（包含本数）的，甲方有权解除合同，乙方无权要求甲方再支付剩余合同款项，并向甲方支付合同总价 30%的违约金。

（三）若乙方更换工作人员，必须提前 7 日向甲方书面报备，经甲方同意后，方可更换。

（四）经过甲方二次组织验收无法通过的，甲方有权拒绝支付合同款项并解除本合同。

（五）如乙方未按合同约定及时进行提供相应服务，甲方可自行组织人员或委托第三方进行维护、解决，因此造成的所有责任、费用由乙方承担，且甲方有权在剩余款项中直接扣除，不足部分，有权向乙方追偿。

（六）驻场人员严格遵守甲方的各项管理规定，未按时按量按质到岗，甲方拒付所有服务费用；如乙方驻场人员变动两次（含）以上，出现一次甲方扣除合同总价的 10%；如乙方驻场人员由于人员变动出现驻场空档期，甲方按照每天 500 元扣除驻场人员空档期费用；服务期内未经学校同意不得随意更换驻场人员，驻场人员的技术能力若不满足学校要求的，服务方必须无条件立即更换，每更换一名技术人员，服务期顺延 30 天；如因乙方驻场人员造成我校网络安全事件（事故）发生，乙方需承担全部责任。

（七）乙方违约而采取的任何补救措施已超过 24 小时都不能弥补甲方受损害的利益情况下，甲方可向乙方发出书面通知，终止全部或部分合同，并由乙方承担违约责任，该违约责任不低于合同总价的 50%。

（八）未经甲方书面同意，乙方不得将本合同项目部分或全部工作分包或转包给第三人。否则，甲方有权解除合同，乙方应按照合同总价的 30%支付违约金，若该违约金无法弥补甲方损失，甲方有权向乙方进行追偿。

（九）在合同履行过程中，非甲方原因导致乙方人员出现人身安全或财产安全事故均由乙方负全部责任，并承担一切损失，甲方不承担任何责任。但由此给甲方造成损失的，乙方应按照甲方的实际损失承担赔偿责任（包括但不限于甲方为此支付的赔偿金、违约金、律师费、诉讼费等）。

（十）甲方有权从乙方合同价款中直接扣除乙方应支付的违约金及赔偿款，不足抵扣的，乙方应在收到甲方通知之日起三日内予补足。

（十一）在本合同履行过程中，因乙方违约行为，给甲方造成损失的，除合同约定违约责任外，甲方有权就其全部损失向乙方追偿。乙方赔偿的全部损失范围包括甲方由此产生的直接损失及追究乙方违约、赔偿责任而产生的律师费、诉讼费、保全费、公证费、交通费等间接损失。

十、争议的解决

合同执行中发生争议的，双方应协商解决，协商达不成一致时，任何一方可向甲方所在地人民法院提起诉讼。

十一、其他

本合同未尽事宜，需经双方共同协商另行签订补充合同或协议，与本合同具有同等法

律效力。

双方确认以本合同上载明的联系地址作为通知送达地址，本合同一方给另一方的通知，均可以书面的形式（信函、传真、电子邮箱）送达至对方联系地址，拒收或因地址变更未通知而无法送达的均视为有效送达。如一方的联系人或地址有变动，需书面向另一方说明，否则，守约方按本合同约定联系方式通知行为有效。

十二、合同订立

（一）本合同自签字、盖章之日起生效。在合同执行期内，双方均不得以随意变更或解除合同。如一方需变更合同，须经另一方书面同意并就变更事项达成一致意见后，方可签订变更协议。若双方就变更事项不能达成一致意见的，提议变更方仍以本合同约定继续履行，否则视为违约。

（二）本合同一式捌份，甲方伍份、乙方贰份、招标公司壹份，具有同等法律效力。签字盖章后生效。

[以下无正文]

甲方：（盖章）西安音乐学院

地址：西安长安中路108号

邮政编码：710061

法定代表人或委托代理人：

开户银行：交通银行西安高新技术产业开发区支行

账号：611301051010149441056

电话：029-88667022

传真：029-88667014

电子邮箱：

签订日期：2025.9.10

乙方：（盖章）西安云唐电子科技有限公司

地址：陕西省西安市高新区丈八一路1号汇鑫中心D座404-2

邮政编码：710065

法定代表人或委托代理人：黄玉玲

开户银行：中国民生银行股份有限公司西安分行营业部

账号：161273248

电话：029-81772968

传真：029-81772968

电子邮箱：329019711@qq.com

签订日期：2025.9.10