服务采购合同

项目名称：陕西省市场监督管理局科技与信息化项目综合业务系统维保项目

甲　　方：陕西省市场监督管理局

乙　　方：上海熙菱信息技术有限公司

签订时间：2026 年 5 月

甲　方：陕西省市场监督管理局

住所地：西安市未央区二环北路东段739号

法定代表人：高晶华

联系方式：029-86138665

通讯地址：西安市未央区二环北路东段739号

传真：029-86138665

乙　方：上海熙菱信息技术有限公司

住所地：上海市青浦区赵巷镇佳杰路99弄2号2层A区2035室

法定代表人：何岳

联系方式：021-61620210

通讯地址：上海市青浦区赵巷镇佳杰路99弄2号2层A区2035室

传真：021-61620219

1 合同说明

1.1 根据陕西省市场监督管理局科技与信息化项目综合业务系统维保项目的竞争性磋商结果，甲乙双方本着相互信任、真诚合作的原则，经充分协商，就乙方为甲方提供服务达成一致意见，依据《中华人民共和国民法典》等相关法律规定以及双方意思真实表示，在平等自愿的基础上签订本合同，以兹共同遵守。

此外，采购/招标文件、响应/投标文件的所有内容是构成本合同不可分割的部分。采购/招标文件、响应/投标文件与本合同不一致之处，以本合同为准。

合同的附件为本合同不可分割的部分，与本合同正文具有同等的法律效力。附件与本合同约定不一致的，以本合同的约定为准。

双方如签订补充协议，补充协议与本合同具有同等效力。

1.2 本合同另有附件：

附件 1：服务费用分项明细。

附件 2：服务内容。

附件 3：保密协议。

2 合同内容

本合同内容为陕西省市场监督管理局科技与信息化项目综合业务系统维保项目。

2.1 本合同的服务期为：2026 年度。（因财政预算批复、省数政局备案及招标采购流程需合理周期，运维服务可能无法无缝衔接。为确保信息系统持续安全稳定运行，原服务商应在本合同到期后，继续提供同等标准的运维服务，直至新服务商确定并完成合同签订。过渡期服务费用由新中标服务商向原服务商据实支付，原服务商须保持服务标准不变、保障事项不减。未尽事宜由甲乙双方另行协商确定。）

2.2 运维方式为：现场运维（现场运维/远程运维/服务类）；

2.3 具体服务内容见附件2。

3 合同金额及付款信息

3.1 服务费用

服务费用总价为人民币:￥575,000.00元 （大写:伍拾柒万伍仟元整)。分项费用明细详见附件1。

实际支付参见本合同3.2，本合同金额为含税金额。本合同产生的一切费用由乙方承担,甲方不再向乙方支付其他任何费用。

3.2 结算方式

具体结算方式为:

1）合同签订之日起7个工作日内，甲方需向乙方支付合同总额的90%作为预付款，即¥517,500.00元（大写：伍拾壹万柒仟伍佰元整）。

2)项目验收合格后7个工作日内，甲方需向乙方支付合同总额的10%，即¥ 57,500.00 元（大写：伍万柒仟伍佰元整 ）。

3.3 甲方开票信息

单位名称：陕西省市场监督管理局

单位地址:西安市二环北路东段739号

纳税人识别号: 11610000MB2964081P

开户行：中国光大银行西安经济技术开发区支行

账　号：78680188000298313

发票类型：普通发票

4 甲乙双方职责

4.1　甲方职责

（1）及时向乙方告知故障现象、错误信息，及时传达运维系统网络安全通报情况，协助乙方做好故障跟踪，为乙方及时、准确地记录、分析和排

除故障提供便利。

（2）为乙方的现场/远程维护提供必要的工作场地和工作条件。在不影响正常业务开展的情况下，为乙方提供维护/修机时间，安排工作人员协助乙方工作。

（3）对乙方工作进行监督和评判。

（4）保护/保密乙方的知识产权。

（5）按本合同规定的时间、方式支付合同款项。

（6）根据有关运维管理制度，对系统修改/新需求进行审定。

4.2 乙方职责

（1）乙方在服务期确保 陕西省市场监督管理局科技与信息化项目综合业务系统 正常运行、稳定可用，及时响应网络安全通报并按要求完成问题整改，严格保障系统网络安全与数据安全，全面履行本合同约定的各项运维服务内容。

（2）乙方派遣 1 名运维人员在服务期内驻场提供服务，办公地点为甲方指定场所，及时响应业务咨询、系统故障处置、日常操作支持等服务需求。驻场团队设项目负责人1名，负责与甲方日常联络、工作协调及问题闭环。驻场人员办公遵守陕西省市场监督管理局信息中心日常管理，运维人员变更需及时向甲方进行书面报告。

（3）乙方保证所提供的服务及相关技术成果不存在任何权利瑕疵（包括但不限于知识产权、数据权属等），如因乙方违反上述保证给甲方及所属单位造成损失的，由乙方承担全部赔偿责任。

（4）乙方应全面履行招标文件、投标文件及本合同中承诺的其他服务事项与工作要求。

5 知识产权归属

5.1 受甲方委托，乙方在运维服务期间开发、定制、完善形成的应用软

件、信息系统代码（含源代码）、运维数据、相关文件及技术文档，其所有权、著作权、使用权及全部知识产权权利均归甲方所有。因本信息系统项目新产生的商业秘密、技术资料、技术诀窍、未公开技术信息及数据资源，所有权与处置权亦归甲方所有。乙方不得擅自使用、许可或转让上述权利，不得泄露相关秘密信息、技术资料与技术诀窍；未经甲方书面同意，乙方不得将上述成果用于本合同以外的任何用途。

5.2 双方确定，因履行本合同所产生的研究开发成果及其相关知识产权权利归属，按下列第（2）种方式处理 ：

（1）甲方享有申请专利的权利。

（2）按技术秘密方式处理。有关使用和转让的权利归属及由此产生的利益按以下约定处理：

①技术秘密的使用权：归甲方所有

②技术秘密的转让权：归甲方所有

③相关利益的分配办法：归甲方所有

双方对本合同有关的知识产权权利归属特别约定如下：归甲方所有。

5.3 乙方不得在向甲方交付研究开发成果之前，自行将研究开发成果转让给第三人。否则，乙方应赔偿给甲方因此造成的全部损失，并将所得利益全部交还给甲方。

5.4 乙方提供给甲方的来自于或属于第三方的软件，具有合法的所有权、版权和使用权，乙方必须将所有授权给甲方的第三方软件的所有权、版权和使用权等书面文件的原件交甲方。

5.5 乙方须保障甲方在使用其产品、服务及其任何部分不受到第三方关于侵犯专利其他知识产权的指控。任何第三方如果提出侵权指控，乙方须与第三方交涉并承担可能发生的一切法律和费用责任。

5.6 甲方对乙方所提供的软件有自行升级的权利。甲方有权利对乙方所

提供的自行开发软件进行升级，升级后的成果属于甲方所有。对原本程序的附加或修改为顺利运行本信息系统，甲方可以根据其实际需要，对乙方所提供的自行开发的软件进行必要的附加或修改；并有权在本信息系统上运行其它的应用软件。

6 网络安全

6.1 乙方应根据合同任务建立相对独立的管理运营技术团队，并指定一名高管作为网络安全负责人，全面落实网络安全主体责任。

6.2 未经甲方书面同意，乙方不得将本合同项下的服务与相关工作转包、违法分包或变相分包。

6.3 本项目涉及的采集数据、业务数据、个人信息及所有数据资源均归甲方所有。乙方不得擅自改变数据用途、不得泄露、传播、转让或许可第三方使用；合同终止或甲方要求时，应按规定完整移交、安全销毁或妥善处理，并出具处理确认记录。涉及个人重要信息的，应当严格遵守《中华人民共和国个人信息保护法》等法律法规及甲方相关管理规定。

6.4 乙方应当关闭系统服务器自动升级功能，升级前应当审核验证补丁包的安全性、适用性、兼容性，同步做好应急处置准备。乙方应当关闭业务终端互联网在线升级功能。乙方对系统升级的应建立分批逐步安装升级策略，验证稳定后实施部署。乙方应当加强开源代码和第三方组件安全测试评估，加强安全软件、外围设备等产品兼容性适配和装机前验证。

6.5 采用远程运维的，乙方应当由专人使用专用终端在专门运维场所和特定网络区域开展，不得通过互联网开展。确需通过互联网开展的，应当使用安全传输模式，采取白名单、按需审批、限时开放等方式实施严格访问控制，采用密码技术建立安全的信息传输通道。

6.6 系统面向内部工作人员使用的功能，乙方应当设置访问策略，使用安全传输模式，采取多因素认证措施。

6.7 乙方应当每季度至少开展一次全面网络安全漏洞扫描与风险排查，及时整改安全隐患，扫描、整改及处置情况须按时向甲方书面报告；未经甲方同意，不得对外披露或向第三方提供。

6.8 乙方应当对系统及数据进行同城和异地备份，定期检查备份系统和数据完整性，开展数据和业务可恢复性测试。按照不低于主系统安全级别的原则，加强备份系统和数据安全防护。

6.9 乙方收到甲方转来网络安全和信息化主管部门的监测通报，应主动配合、积极采取相应措施，进行整改，保障系统正常运行。

6.10 发生可能影响本项目网络安全的重大事项，包括企业法定负责人、网络安全负责人、核心技术人员变更，以及经营调整、合并分立、重组并购等，应提前书面报告甲方，并采取有效保障措施确保系统与数据安全。

7 违约责任

7.1.合同生效后，甲乙双方应按合同规定认真履约，一方违反合同约定应当承担违约责任。

7.2.乙方若未按合同约定期限提供服务，每逾期一日，向甲方支付违约金1000元。逾期超过15日的，甲方有权解除本合同，乙方按照合同总额10%支付违约金，乙方就甲方损失应当承担全部赔偿责任。

7.3.除不可抗力原因外，如遇下列情况之一者，甲方有权单方面解除合同，乙方应当向甲方支付合同总价款10%的违约金，并赔偿因此给甲方造成的全部损失。

（1）合同签订后不能按合同时限要求提供服务。

（2）所供服务不合格或与合同不符。

（3）不能按合同履约。

（4）甲方要求乙方提供服务，经甲方要求24小时内无响应，或48小时内不能提供服务方案或服务的，或者经甲方催促后仍不能整改或提供服务

不达标的。

7.4.乙方对所提供服务出现的问题推托、拖延，未在约定时间内做出服务响应的，每逾期一日按合同总金额0.5%支付违约金。

7.5.合同履约过程中，甲方应积极配合乙方进行验收以及验收前的外围配套等工作。

7.6.本合同履行过程中，任意一方未及时履行相关义务，经守约方催告后仍未履行的，守约方可于催告期满后解除本合同，由此产生的相应损失，由违约方承担。

7.7.未经甲方许可，乙方不得擅自将本合同约定的全部或部分义务转让给第三方，否则甲方有权解除本合同，乙方应当向甲方支付本合同总价款10 %的违约金。同时，给甲方造成损失的，乙方应承担全部赔偿责任。

7.8.乙方应当对本合同履行过程中获取的甲方相关数据及资料承担保密义务，保密期限为长期。乙方违反本合同约定的保密义务的，应当向甲方承担本合同总价款10%的违约金并立即采取补救措施。同时，甲方有权解除本合同。同时，给甲方造成损失的，乙方应当承担全部赔偿责任。

8 不可抗力

8.1 不可抗力是指本合同生效后，发生合同订立时不能预见、不能避免，并不能克服的客观情况，如地震、台风、水灾、战争等，致使直接影响本合同的履行或不能按约定的条件履行。

8.2 发生不可抗力的一方应立即通知对方，并在十五天内提供不可抗力的详情及将有关证明文件送交对方。

8.3 发生不可抗力事件时，甲乙双方应协商以寻找合理的解决方法，双方不可放任不可抗力事件损害后果。

8.4 如不可抗力事件持续三十天时，甲乙双方应友好协商解决本合同是否继续履行或终止的问题。

9 合同生效与期限

9.1 除非另有说明，本合同经甲乙双方法人代表或由法人代表授权的全权代表签字、加盖合同章后生效。

9.2 本合同由陕西省市场监督管理局（甲方）与 上海熙菱信息技术有限公司 （乙方）签订，合同文书共6份，其中甲方4份，乙方2份。

9.3 合同执行期间，甲、乙双方均不得随意变更或解除合同。本合同的任何修改和变更均以双方协商一致的书面文件为准。

9.4 本合同自甲乙双方权利义务履行完毕后，合同自动终止。

10 争议解决

10.1.因本合同及合同有关事项发生的争议，由甲乙双方友好协商解决。协商不成时，可以向有关组织申请调解。合同一方或双方不愿调解或调解不成的，应向甲方所在地人民法院提起诉讼。

10.2.如甲乙双方有争议的事项不影响合同其他部分的履行，在争议解决期间，合同其他部分应当继续履行。

11 双方约定本合同其他相关事项

11.1.合同的变更

政府采购合同履行中，在不改变合同其他条款的前提下，甲方可以在合同价款10%的范围内追加与合同标的相同的服务，并就此与乙方协商一致后签订补充协议。

11.2.合同的中止

（1）合同履行过程中因供应商就采购文件、采购过程或结果提起投诉的，甲方认为有必要的，可以中止合同的履行。

（2）合同履行过程中，如果乙方出现以下情形之一的：1. 经营状况严重恶化；2. 转移财产、抽逃资金，以逃避债务；3. 丧失商业信誉；4.有丧失或者可能丧失履约能力的其他情形，乙方有义务及时告知甲方。甲方有权

以书面形式通知乙方中止合同并要求乙方在合理期限内消除相关情形或者提供适当担保。乙方提供适当担保的，合同继续履行；乙方在合理期限内未恢复履约能力且未提供适当担保的，视为拒绝继续履约，甲方有权解除合同并要求乙方承担由此给甲方造成的损失。

（3）乙方分立、合并或者变更住所的，应当及时以书面形式告知甲方。乙方没有及时告知甲方，致使合同履行发生困难的，甲方可以中止合同履行并要求乙方承担由此给甲方造成的损失。

（4）甲方不得以行政区划调整、政府换届、机构或者职能调整以及相关责任人更替为由中止合同。

11.3.合同的终止

（1）合同因有效期限届满而终止；

（2）乙方未按合同约定履行，构成根本性违约的，甲方有权终止合同，并追究乙方的违约责任。

11.4.涉及国家利益、社会公共利益的情形

政府采购合同继续履行将损害国家利益和社会公共利益的，双方当事人应当变更、中止或者终止合同。有过错的一方应当承担赔偿责任，双方都有过错的，各自承担相应的责任。

11.5 验收标准

（1）项目服务期结束后，由甲方的业务需求部门提出验收申请，甲方委托代理人所在部门组织需求部门、专家和第三方监理机构进行验收。

（2）验收文件应包括技术方案、服务记录、服务报告、用户意见书、第三方监理报告等，以及采购文件（如有）、响应文件（如有）相关资料。

（3）项目验收通过后，所有参加验收人员及第三方监理机构签署项目通过的验收意见。

11.6 税费

（1）根据现行税法，国家或地方政府向甲方征收的与履行本合同有关的一切税费由甲方支付。

（2）根据现行税法，国家或地方政府向乙方征收的与履行本合同有关的一切税费由乙方支付。

11.7 保密义务

（1）保密信息范围与使用限制

甲方向乙方提供的所有非公开资料、文件，以及在项目执行过程中产生的所有数据资源、技术成果，均属于甲方保密信息。乙方及项目组成员仅可将其用于本合同约定的系统运维与维护工作，不得用于任何其他目的。

（2）人员管理与保密责任

乙方应确保项目参与人员相对固定，入职前须对运维人员进行背景审查，并与其签署合法有效的保密协议。乙方人员应严格遵守保密纪律，妥善保管甲方资料与数据，严禁以任何形式（包括但不限于私自下载、拷贝、复制、传播、泄露、遗失）对外披露或外泄。

（3）泄密责任与损害赔偿

若因乙方技术实力、管理不善或乙方人员原因，导致技术资料、业务数据、业务资料及关键源代码发生泄露、丢失或被非法获取的，乙方须立即启动应急补救程序，并承担相应的法律责任；因此给甲方造成损失的（含直接损失与间接损失），乙方应承担全部赔偿责任。

（4）保密期限

本合同项下的保密义务具有持续性。无论本合同是否变更、解除或终止，乙方的保密义务始终有效；保密期限为长期，自合同生效之日起计算。

（5）乙方成果的保密保护

乙方提供给甲方的技术资料、文档及其他成果，甲方负有保密义务。未经乙方书面许可，甲方不得将其用于本合同约定以外的传播、复制或商业目

的，否则须承担相应法律责任，并赔偿乙方因此遭受的经济损失。

甲方：陕西省市场监督管理局（盖章）

法定代表人：高晶华

地址：西安市未央区二环北路东段 739 号

委托代理人：丁妍

联系电话：029-86138665

签字日期：2026 年 5 月 19 日

乙方：上海熙菱信息技术有限公司（盖章）

法定代表人姓名：何岳　　法定代表人性别：男

乙方所在区：上海市青浦区

乙方详细地址：上海市青浦区赵巷镇佳杰路 99 弄 2 号 2 层 2035 室

乙方性质：☐大型　☑中型　☐小型　☐微型　☐其他

乙方特殊性质：☐监狱企业　☐残疾人福利企业　☐其他

乙方收款账户开户行：招商银行上海张江支行

收款账户账号：1219 0822 9110 302

法定代表人授权代表：何岳

法定代表人联系电话：021-61620210

签字日期：2026 年 5 月 19 日

附件 1：

服务费用分项明细

单位：元

序号	服务类别	服务内容	金额（元）	备注
1	软件运维	日常技术支持	325000	
2		故障处理		
3		定期巡检		
4		数据处理		
5		业务应用软件的运行监控		
6		中间件运维		
7		数据库软件运维		
8		操作系统软件运维		
9	其他运维	数据采集	250000	
10		数据处理		
11		数据服务		
12	合计		575000 元	

附件 2：

服务内容

一、项目概述

1.项目背景

2018 年 11 月，陕西省市场监督管理局正式挂牌，根据《陕西省机构改革方案》将省工商行政管理局、省质量技术监督局、省食品药品监督管理局的职责，以及省发展和改革委员会的价格监督检查与反垄断执法职责，省商务厅的经营者集中反垄断执法职责，省盐务管理局食盐市场安全监管职责等整合，组建省市场监督管理局，作为省政府直属机构。

陕西省市场监督管理局科技与信息化处承担着全局拟订并组织实施市场监督管理科技发展规划。负责重大科研课题的组织、论证、引进、交流合作和成果推广工作。负责本系统技术机构及省级质检中心能力建设及规划，指导基层技术机构能力建设。负责市场监督管理信息化建设工作的职责。

2.运维服务情况

在数字化时代，软件系统已成为业务运营的核心。软件的稳定性、可用性和性能直接影响用户体验和业务成果。因此，对软件运维的需求分析至关重要，以确保软件系统能够持续满足业务需求并保持最佳状态。

需要对陕西省市场监督管理局科技与信息化项目综合业务系统提供的运维服务包括：操作系统软件、数据库软件、中间件、业务应用软件的运行监控、数据处理、定期巡检、故障处理、日常技术支持等服务。

二、技术要求

1.服务范围

软件运维服务、其他运维服务。

2.服务期限

2026 年度。

3.服务目标

陕西省市场监督管理局科技与信息化项目综合业务系统维保项目以“零故障”为服务目标，确保系统7×24小时稳定运行，且制定切实可行运维保障体系，一但系统出现故障，保证在最快的时间内排障。保障系统正常运行，不影响客户使用。

同时派驻现场运维人员，做好数据服务、培训等其他维护工作。

具体达到的目标如下：

1.系统可用性：99.99%

2.用户满意度：98%

3.无重大质量事故，无重大顾客投诉。

4.故障处理时间：见下表1-1

表1-1故障处理时间要求

故障级别	远程响应	现场响应	故障解决时间
普通故障	立即响应	2小时内到现场	到达现场后<3小时
重大故障	立即响应	1小时内到现场	到达现场后<2小时
特大故障	立即响应	30分钟内到现场	到达现场后<1小时

4.服务内容

第1部分 软件运维服务

对陕西省市场监督管理局科技与信息化项目综合业务系统提供的服务包括：操作系统软件、数据库软件、中间件、业务应用软件的运行监控、数据处理、定期巡检、故障处理、日常技术支持等服务。

第2部分 其他运维服务

派驻现场运维人员，做好数据服务、培训等其他维护工作。

一、软件运维服务内容

1.技术支持及咨询服务

驻场服务人员要为市监局用户提供信息化项目和科研项目的上报、业务查询等操作指导服务。

驻场服务人员要为全省各级市场监管用户提供各业务模块使用咨询；机构改革过程中，各机构调整及名称变更的需求处理；日常监管及风险和信用评定使用不熟练的操作指导；用户信息调整及维护。

对系统用户信息进行维护和修改，添加系统用户、更改系统用户信息、权限，负责系统中管理人员、操作人员、监督人员名单的调整，以及数据同步。

驻场运维服务人员在处理日常问题时应及时记录和梳理各类问题的来源、处理结果、处理人员等信息，并形成日志按期汇报，以备查验。

2.问题收集及反馈服务

驻场服务人员不仅要在日常运维工作中梳理和反馈用户提出针对系统的不同问题，还应定期与其他业务处室及时沟通，为系统使用过程中遇到的问题进行合理化的处理，并提供相关信息化建设咨询服务，让系统建设更切合业务实际，让规划更具有持续性和目标性。

3.系统支撑资源监测巡检及常维护

运维提供方需利用已有或自建的相关自动监控工具实时了解并合理利用工具监控各业务模块的运行状况、数据情况、传输情况，及时获取相关资源的运行情况，关注相关资源的网络速率、存储剩余、资源使用率。根据监控情况提前获知系统运行的瓶颈及相关资源阈值，及时汇报相关情况至相关负责人，以便于提前做好应急预案，保障系统的稳定可持续运行。系统支撑软硬件主要包括PC服务器、存储、网络、安全设备及数据库软件、中间件

等基础软硬件设施。

（1）服务器巡检及维护

服务器系统主要包括信息处目前在用的各类服务器：数据库服务器、应用服务器、WEB/网管/备份服务器、门户网站、防病毒服务器等。具体服务内容包括：

·服务器硬件状态检查

·服务器硬件安装与调整

·服务器设备事件管理服务

运维团队根据服务器的情况制订相应的事件管理文档，由现场服务人员对服务器发生的事件进行记录、跟踪与分析，通过对事件的分析，及时发现服务器中存在的潜在问题，并进行解决或提出相应的解决方案。

（2）服务器性能监控

要求运维团队每天由现场服务人员根据制定的性能监测模板对服务器的性能监控，监控的参数为服务器的CPU、memory、hdd、network，并根据各服务器的应用情况，分析出服务器性能的基本基准线。

（3）应用维护

要求运维团队现场服务人员对这些应用进行定期的维护，对防病毒软件的防护状态与更新情况进行每天检查。

（4）存储设备维护

当系统出现异常数据丢失时，协同应用厂商，在信息处的授权下，要求运维团队现场服务人员对相应的备份数据进行数据恢复，以快速保证与恢复客户的应用。

（5）备份数据整理

由于目前备份数据没有明确的管理制度，备份数据管理程无序化状态，对于备份数据的保存声明周期没有周密的限定计划，造成备份数据占用大量的存储空间，要求运维团队现场服务人员根据备份和存储数据的情况，提出数据整理频率计划，并信息处进行数据的整理。

（6）存储设备运行维护

要求运维团队现场服务人员对存储设备硬件状态监控，问题及时处理。

（7）数据库系统维护

根据目前综合业务系统运行的情况来看，系统每天都会产生大量的结构性数据，各业务模块之间数据的交换调用频繁，业务逻辑复杂。因此需要对数据库的运行情况和生产持续关注和优化，也要有成熟的容灾备份方案，提高数据库的高效和稳定性。

提供对系统数据库运行维护服务，包括主动数据库性能管理，数据库的主动性能管理对系统运维非常重要。通过主动式性能管理可了解数据库的日常运行状态，识别数据库的性能问题发生在什么地方，有针对性地进行性能优化。同时，密切注意数据库系统的变化，主动地预防可能发生的问题。

数据库运行维护服务还包括快速发现、诊断和解决性能问题，在出现问题时，及时找出性能瓶颈，解决数据库性能问题，维护高效的应用系统。

数据库运行维护监控的基本服务内容包括：

序号	服务模块	内容描述
1	数据库 7*24 电话支持服务	1.每周 7 天，每天 24 小时支持中心电话，电子邮件答询，以满足业务发展的需要。 2.产品技术专家直接同客户对话，帮助解决客户提出的疑难问题。 3.根据问题的严重程度，将优先解决客户认为是关键而紧急的任务。 4.对客户提出的一般性问题进行技术咨询、指导。 5.定期的客户管理报告，避免问题再度发生。
2	数据库产品现场服务响应	1.数据库宕机。 2.数据坏块。 3.影响业务不能进行的产品问题。 4.软件产品的更新及维护。

3	数据库产品系统健康检查	1.对系统的配置及运作框架提出建议，以帮助您得到一个更坚强可靠的运作环境降低系统潜在的风险，包括数据丢失、安全漏洞、系统崩溃、性能降低及资源紧张检查并分析系统日志及跟踪文件，发现并排除数据库系统错误隐患检查数据库系统是否需要应用最新的补丁集。 2.检查数据库空间的使用情况。 3.协助进行数据库空间的规划管理。 4.检查数据库备份的完整性。 5.监控数据库性能。 6.确认系统的资源需求。 7.明确您系统的能力及不足。 8.优化数据库的表现。 9.通过改善系统环境的稳定性来降低潜在的系统宕机时间。
4	数据库产品性能调优	1.分析用户的应用类型和用户行为。 2.评价并修改数据库的参数设置。 3.评价并调整数据库的数据分布。 4.评价应用对硬件和系统的使用情况，并提出建议。 5.利用先进的性能调整工具实施数据库的性能调整。 6.培训用户有关性能调整的概念。 7.提供用户完整的性能调整报告和解决方法。

4.中间件维护

中间件(Middleware)负责管理Web服务器和数据库服务器之间的通信并提供应用程序服务,它使基于Web的应用程序得以运行,用户可以正常访问。它负责管理用户对应用程序的访问，执行应用程序中的业务逻辑，对计算机资源、网络通信进行管理。随着Web类应用的普及，中间件也成为应用程序

部署开发时不可或缺的一部分。它可以满足用户高并发、分布式计算的需求。伴随着业务量、数据量的增长，中间件运行过程中会遇到各种问题。运维人员需要指定中间件维护计划，并按照计划进行维护，保证中间件的正常稳定运行。

本项目对Kafka、ElasticSearch、Redis等中间件的日常维护管理和监控工作，提高对中间件平台事件的分析解决能力，确保中间件平台持续稳定运行。中间件监控指标包括配置信息管理、故障监控、性能监控。

可以概括为以下几个方面：

（1）Kafka日常维护管理

1）监控和报警设置：

实施实时监控，洞察Kafka的健康状况，包括资源使用监控、性能监控等。

监控指标包括集群的负载、磁盘使用率、消息吞吐量等关键性能指标。

2）集群业务影响分析：

分析集群的各个Topic涉及的业务使用场景，跟踪管理特别是对于核心业务链路直接或间接依赖的Kafka集群。

3）集群稳定性观察：

监控、巡检结果风险感知，及时与中间件运维团队保持同。

（2）ElasticSearch日常维护管理

1）快照保留：

定期执行快照保留任务，确保数据的备份和恢复能力。

（3）Redis日常维护管理

1）监控和报警：

监控Redis的性能和状态，使用监控工具如Grafana、Prometheus等进行实时监测和报警。

2）备份和恢复：

定期进行数据备份，使用Redis自带的RDB快照功能或者AOF持久化功

能进行数据备份。

3）性能调优：

根据业务增长调整Redis配置参数，如最大连接数、最大内存限制、缓存策略等，以优化性能。

4）安全性管理：

设置访问密码、限制访问IP、关闭不必要的命令等方式来加强Redis的安全性，并定期更新版本以修复安全漏洞。

5）日志管理：

配置日志级别、输出、轮转，以及实时日志监控和日志聚合分析，以洞察系统状态。

6）故障排查和性能优化：

出现问题时，通过查看Redis的日志、监控数据来分析和定位问题的原因，并进行性能优化。

5.应用系统监测巡检及维护

通过监控工具及其他科学的方法，及时获取系统运行的重要参数，为系统提高准确可靠的基础信息支撑

通过对应用系统的维护，分析用户的不断更新的需求，分析应用系统对服务平台性能的要求，提出系统优化扩容解决方案，保障应用系统的处理服务性能。

对业务管理系统健康状态检查与分析报告；

对系统用户信息进行维护和修改，添加系统用户、更改系统用户信息、权限，负责系统中管理人员、操作人员、监督人员名单的调整，以及数据同步。

（1）受理、处理用户反馈的各类问题

系统是对内的项目审批的重要系统，受理、处理各类咨询、建议、问题等问题，受理需做好问题登记、解决、反馈等事项，并将各类问题进行汇总，

形成常见问题知识库，供用户进行查阅。

（2）系统数据的维护

业务处理对数据的要求是不断发生变化的，除了系统中业务数据的定期正常更新外，还有许多数据需要进行不定期的更新，或随环境或业务的变化而进行调整，以及数据内容的增加、数据结构的调整。此外，还包括数据的定时与不定时的备份与恢复等。

（3）数据备份

为防止不能预料的系统故障或用户不小心的非法操作，对系统进行安全备份。除了对全系统进行定期的备份外，还对修改过的数据进行每周一次全量备份，每天一次增量备份。同时，将修改过的重要系统文件存放在不同的服务器上，以便出现系统崩溃时，可及时地将系统恢复到正常状态。

（4）日常系统的监控与处理

每日不定时查看系统运行日志，记录下所有用户使用系统的情形，包括最近登录时间、使用的账号、进行的活动等，并生成报表，通过对报表进行分析，了解系统是否有异常现象，对于异常及时进行处理。

（5）系统升级工作

做好系统升级前的用户现场测试工作，保证系统升级后不会出现新的问题。同时做好应用系统升级前的备份工作。

（6）系统安全防护工作

系统安全防护一是保证系统正常运行，二是防止系统及数据被非法利用或破坏。

（7）月度运行维护工作

对当月系统产生的故障进行总结分析纪录存档，并制定相关维护措施，保障系统可靠、安全运行。

对当月的数据库进行优化，并做详细的纪录。

（8）季度、年度运行维护工作

对系统设备每年进行四次（3月、6月、9月、12月）巡检，并写出详

细的巡检报告。

根据系统业务发展情况，制定系统扩容计划。

6.应用系统性能调优

随着综合业务系统用户量和业务数据的增加，运维提供商要及时了解应用系统的性能情况，基于相关资源及监控数据，对数据库、前台页面访问速度、后台处理速度等进行性能瓶颈分析并形成调整方案上报主管部门。

7.应急保障服务

提供两会应急保障、领导视察汇报，网络应急事件处理等特殊保障服务，事前安排技术人员对软硬件进行全面巡检，并根据实际情况安排师提供现场值班技术支持服务。

8.数据及应用安全

根据业务调整，做好系统数据维护，涵盖组织信息、人员情况、业务数据、科研项目信息等，保障数据安全。及时备份系统应用数据和业务数据库，做好容灾与安全保密，防止企业及政府数据泄露。对运维服务人员开展安全保密培训，减少数据泄露环节，保护科技与信息化申报管理相关数据安全。

建立健全系统安全保密制度，提升运维工作的风险防控能力。具体包括：一是保障数据安全与保密性，二是强化运维人员的安全保密意识培养。

风险评估与安全加固工作贯穿于信息系统的全生命周期各阶段。在运行维护阶段，需持续开展风险评估，以识别系统所面临的动态变化的风险与脆弱性，并通过实施安全加固措施，采取有效的安全干预，从而确保既定安全目标得以实现。

9.容灾备份及恢复

系统数据需实时进行本地和异地备份容灾，确保意外发生时业务系统不受影响；敏感数据采用加密技术，降低核心敏感信息泄露风险。

系统容灾备份工作需涵盖数据库、代码库、文件库及过程资产等多个层面，并应建立完善的容灾机制与责任体系。须定期检验备份文件的可恢复性与完整性，同时按计划组织容灾恢复演练，以确保系统容灾措施得到切实执行。

10.服务报告

（1）月度检查报告

每月对各系统及设备进行检查，进行安全系统、防病毒系统检查，进行漏洞扫描，并对检查中存在的故障及安全隐患进行处理。每月第一周向用户单位提交上月的《月度巡检报告》，报请用户单位审批签署。

（2）季度检查报告

每季度对由维护团队的专业维护队伍对所有设备进行安全评估和风险分析，提交完整的安全状况评估报告，分析存在的安全漏洞情况，提出《整改方案和建议》。

（3）年度检查报告

每年由维护团队组织相关的专家（含硬件和软件）对整个系统进行安全检查，对每个硬件设备使用状态进行风险评估，并对下一年可能存在的问题进行风险预测，对每个设备的状态出具使用报告。

二、数据处理服务

为用户提供数据相关的支持与服务，包含数据采集、数据处理、数据服务。

1.整体设计

围绕数据服务目标，按照“以服务目录为基础，以闭环管理为核心，敏捷响应规范服务；以绩效目标为导向，保证服务质量进度”的思路，建立长效数据运营服务机制和服务体系。编制数据运营服务目录，定义服务项的服务内容、服务输出及输出物标准、使得服务在执行上能够标准统一和可重复。

以闭环管理为核心，敏捷响应规范服务。从服务工作方案制定、服务任务发起、过程实施及监控、服务验收考核四个方面实现运营闭环管理，针对所有服务任务的前端接收、执行转化、跟踪落实和成果输出的全过程进行闭环式管理。同时，快速响应数据运营服务的需求，根据任务类别细分不同的服务任务类型，制定具体的数据运营服务过程管理流程，规范运营服务。

设计统一数据服务接口，支持跨业务、跨数据库数据访问，提供API接口文档、数据集及资源接入白皮书，方便各部门调用，按数据分级权限进行访问控制，确保数据安全。同时，建立数据治理机制，保障数据的准确性、一致性、完整性和可用性，对数据进行清洗与预处理。此外，遵守法律法规，严格控制数据使用范围和期限，防止数据泄露。

2.数据共享

（1）API共享：通过API（应用程序接口）共享数据，API统一集成到共享平台，授权用户或组织可使用API访问和使用数据。

（2）数据融合共享：将数据融合结果共享给有使用需求的组织或个人。

3.数据维护

建立数据维护制度：制定数据维护制度，明确责任与流程，建立数据管理部门或团队全面管理和维护数据。

定期清洗更新数据：定期对数据清洗和更新，删除重复、错误或无效数据，更新已有数据的变更信息与最新状态。

定期进行数据备份和恢复：定期对数据进行备份防丢失损坏，故障或灾害时及时进行数据恢复。

实施数据安全措施：采取加密、权限控制、访问审计等措施确保数据的安全和保密。

采用数据质量管理工具：用工具检测监控数据质量，及时发现数据质量问题并进行处理。

持续更新数据标准和规范：定期对数据标准和规范进行更新和优化，适应业务与技术发展的变化。

4.服务交付成果

针对数据集对外提供一组多种类型的接口服务，并根据不同用户角色的需求开展满足不同SLA的数据共享需求。一组多种类型的接口服务包括：样例数据接口、Json、Xml等。

5.运维制度与规范

第一章 总则

第一条 制定目的

为保障本项目信息系统安全稳定运行，规范运维服务流程，明确服务标准与责任边界，为陕西省市场监督管理局提供高效、专业、可靠的技术支持与服务，特制定本制度。

第二条 适用范围

本制度适用于项目全生命周期内的所有运维服务活动，涵盖系统故障处理、日常维护、应急响应、技术支持等相关工作，服务提供方及用户方相关人员均需遵守。

第二章 服务原则与核心制度

第三条 故障优先原则

以快速处置系统故障、保障系统安全稳定运行及业务畅通为核心首要原则，全力支撑应用系统开发及后期系统集成全流程工作，秉持 “客户为中心” 服务理念，最大限度协助用户，最短时间内解决故障。

第四条 快速响应原则

组建专门IT服务团队，针对系统故障及用户需求提供快速现场响应与远程支持，确保服务时效。

第五条 一站式服务原则

涵盖故障受理、远程技术支持、现场排障、故障原因分析、问题闭环等全流程服务，为用户提供便捷高效的解决方案。

第六条 流程化管控原则

结合 ITIL 标准及电信级保障维护经验，建立标准化服务流程，明确各环节责任分工，实现闭环管控。

第七条 安全保密制度

严格执行安全保密规定，妥善保管项目相关资料、系统数据及用户信息，严禁泄露任何涉密内容，确保信息安全。

第八条 绩效考核与 SLA 落实制度

将服务质量指标（SLA）纳入团队及个人绩效考核，明确服务标准、责任到人，确保服务质量达标。

第九条 变更管理原则

高效、灵活响应用户合理变更需求，同时执行严格的变更审批流程，评估变更对系统性能、稳定性的影响，避免引发系统故障。

第三章 服务受理规范

第十条 受理渠道

服务期内，用户可通过以下方式提交服务申请，项目经理负责统一受理协调：

现场维保受理：现场维保人员第一时间接收服务申请，提供基础设施软件、应用系统软件、安全系统等维护服务，并依托三线支撑体系保障服务质量；

报修电话受理：提供西安市本地 7×24 小时热线服务，同步提供远程技术支撑；

传真受理：办公时间及重大节日提供即时传真响应服务，及时处理用户书面申请；

在线及邮件受理：开通在线服务通道及专用邮箱，及时接收并回复用户服务需求。

第十一条 受理要求

服务受理人员需详细记录用户信息、问题描述、需求内容、提交时间等关键信息，形成服务工单，确保信息完整、可追溯。

第四章 响应时效标准

第十二条 维保期响应要求

提供1人现场常驻服务，实现7×24小时现场响应；

系统故障响应时间不超过30分钟；

对于疑难问题，30分钟内协调二线技术人员提供支持，支持人员1小时内抵达现场排查原因，2小时内出具解决方案，并持续工作至故障完全消除、系统恢复正常服务；

提供24小时故障报告支持服务，通过传真、电话等多渠道确保及时响应。

第五章 突发事件应急响应机制

第十三条 应急保障体系

项目经理及项目维护经理提供7×24小时通讯畅通保障，确保突发事件第一时间对接；

建立常设虚拟专家组织，定期熟悉项目IT环境、系统配置及相关文档，为应急响应提供技术支撑。

第十四条 应急响应流程

现场人员10分钟内响应突发事件，立即开展初步处置；

需额外技术力量支持时，服务方30分钟内启动应急响应，技术支持工程师1小时内抵达现场；

2小时内完成故障解决；当场无法处理的，迅速转交项目组相关负责人，持续跟进直至问题闭环。

第六章 重要时刻值守服务

第十五条 服务内容

针对用户确认的重大活动、特殊时期等重要时刻，提供维护组现场全过

程值守支持服务，实时监控系统运行状态，及时处置突发问题，保障系统稳定运行。

第十六条 值守要求

值守人员需提前到位，熟悉现场环境及系统情况，全程在岗，做好值守记录，确保重要时刻服务不间断。

第七章 文档管理与技术交流规范

第十七条 文档交付

项目全流程中，服务方需按时向用户提供电子文档与纸质文档各一份。

第十八条 技术交流

适时组织专题信息技术交流活动，分享系统运维经验、技术要点，解答用户方疑问，协助用户提升系统操作及维护能力。

第八章 无推诿服务承诺

第十九条 承诺内容

无论系统故障由哪一方原因导致，服务方均在第一时间派员到场处置，全力排查问题、消除故障，不推诿、不拖延，保障用户业务正常开展。

陕西省市场监督管理局科技与信息化项目综合业务系统维保项目考核表

单位：上海熙菱信息技术有限公司　　年　月　日

类别	评分标准	得分
服务态度(20分)	每次服务态度都很好：20分	
	服务态度比较好偶尔出现不好状态：1—19分	
	服务态度一般经常不理睬甲方需求：0分	
综合技术能力（20分）	所有出现的问题都能解决：20分	
	大部分出现的问题能解决：10—19分	
	部分出现的问题能解决：1—9分	
	无法解决出现的问题：0分	
响应时间（20分）	在甲方提出故障维护请求后，实时给出解决方案：20分	
	在甲方提出故障维护请求后，30分钟内给出解决方案：10—19分	
	在甲方提出故障维护请求后，12小时内给出解决方案：1—9分	
	在甲方提出故障维护请求后，无响应：0分	
问题解决时间（20分）	问题解决时间<30分钟：20分	
	30分钟<问题解决时间<6小时：15—19分	
	6小时<问题解决时间<24小时：4—14分	
	问题解决时间>24小时：0—3分	
主动服务能力（20）	合同期有4次以上主动向甲方处征求意见，主动修改软件中存在的问题并主动告知甲方注意事项：20分	
	合同期有2到3次以上主动向甲方征求意见，主动修改软件中存在的问题并主动告知甲方注意事项:12—19分	
	合同期有2到3次以上主动向甲方征求意见，能修改软件存在的问题：7—11分	
	合同期没有主动与甲方沟通，但是主动修改软件中存在的问题并告知甲方注意事项:1—6分	
	合同期没有主动与甲方沟通，也不修改软件中存在的问题：0分	
总分		
意见和建议		

附件 3：

保 密 协 议

甲方（管理部门）：陕西省市场监督管理局

统一社会信用代码：11610000MB2964081P

法定代表人：高晶华

地址：西安市二环北路东段 739 号

联系方式：029-86138665

乙方（服 务 方）：上海熙菱信息技术有限公司

统一社会信用代码：91310000733341232N

法定代表人：何岳

地址：上海市青浦区赵巷镇佳杰路 99 弄 2 号 2 层 A 区 2035 室

联系方式：021-61620210

依据《中华人民共和国民法典》《中华人民共和国网络安全法》《中华人民共和国数据安全法》、《中华人民共和国保守国家秘密法》《中华人民共和国个人信息保护法》等法律法规，为规范陕西省市场监督管理局所涉信息化项目实施服务全过程管理，确保市场监管数据安全，双方遵照平等、自愿、协商一致的原则签订本保密协议。

一、保密义务的来源

基于甲乙双方合作推进“信息化项目”的需要，乙方为甲方提供信息化建设服务。乙方在甲方管理下，陕西省市场监督管理局信息化建设工作按照《陕西省市场监督管理局信息化项目建设管理办法》、《陕西省市场监督管理局数据工作管理办法》、《陕西省市场监督管理局网络与信息安全应急预案》、《陕西省市场监督管理局关于进一步加强省局业务系统数据安全管理工作的通知》、《陕西省市场监督管理局办公室关于进一步加强数据安全防护的通知》等要求，乙方在甲方管理下为甲方提供信息化项目建设或维保服务，依据项目合同派遣技术人员或设定驻场人员。甲方作为披露方向乙方披露部分保密信息，乙方作为接收方须严格遵守本协议约定的保密义务。

二、保密义务

1.乙方对涉及甲方的以下保密信息承担保密责任：

（1）信息化项目建设或提供服务过程中获知的政策文件、总结报告、会议纪要、工作报表、业务信息等;

（2）依托信息化手段生成的数据资料、安全防护程序;

（3）软、硬件结构化数据及非结构化数据。包括但不限于信息系统涉及的数据库、服务器、网络线路配置，网络系统拓扑图、数据结构、技术参数，开发程序代码、日志信息、公民个人信息等;

（4）乙方代为甲方测试应用的管理员账号、密码，服务器、交换机、路由器等设备的配置信息，链接方式及甲方用户名、口令。

2.具体要求：

（1）乙方保证所有保密信息独立用于项目有关的用途，不得用于项目以外的任何用途，不得运用保密信息进行其它研发拓展，不得私自将保密信息通过存储介质、网络等途径进行转存、传播、

售卖和处理。确有需要，应以书面方式向甲方报批申请。

（2）乙方服务过程中生成的源代码、数码、影像、软件及数据资料包括知识产权在内的一切权利均属甲方所有。不得运用甲方服务对象名义发表虚假信息。

（3）乙方服务过程中对任何硬件网络环境配置、软件系统变更操作，须通过书面申请，甲方批准授权后方可开展工作及终结报备。

（4）乙方服务过程中系统硬件设备送检、外修，必须经甲方书面批准授权后实施，并负责做好密级保护，确保调整、变更、送检、外修等工作中数据资料的保密要求。

（5）乙方驻场人员拟调离或离职时，其工作中使用或涉及归属甲方的电脑、光盘、存储设备及数据等必须返还甲方或经甲方审批销毁数据，确保之后不得外泄。

（6）乙方依照本协议约定执行保密信息管理，并提供安全可靠的保密机制、措施及技术手段，做好对信息化项目实施人员的保密教育及安全背景审查，确保系统安全及驻场保密教育落实。乙方违反本协议约定，甲方有权随时终止合作关系。

（7）乙方未履行本协议导致保密信息被盗用、泄露、损毁、丢失等，应承担因此对甲方造成的经济损失和刑事、行政法律责任。

三、保密期限

乙方保密义务的履行期限为：自本协议签订之日起永久保密。

除非甲方通过书面通知明确说明对本协议所涉及的某项保密信息予以解密或同意共享，乙方必须按照本协议所承担的保密义务对保密信息进行保密。

四、违约责任

乙方保证履行协议义务，对保密信息妥善保管，并对保密期间

发生的以下事项承担全部责任，因此造成甲方损失的，乙方应负责赔偿：

1.保密信息被盗、泄露，或者其他方式的泄露及或毁损、灭失；

2.任何根据本协议有权从乙方获得保密信息的员工（包括但不限于现有员工及原员工）、股东、高管、顾问和/或咨询人员等对保密信息未经授权的披露；

3.因乙方及其参与服务工程的员工原因，造成信息和网络系统遭受攻击、篡改、运行故障等网络安全事件；

4.乙方违反本协议“保密义务”章节任一条款，或因乙方缘故发生其它依据有关规定可视为泄密事件等的事项。

乙方未履行或未完全履行本协议下的条款均构成违约，应赔偿甲方全部损失。本协议中的全部损失包括但不限于对守约方所造成的直接损失、可得利益损失、守约方支付给第三方的赔偿费用/违约金/罚款、调查取证费用/公证费/鉴定费用、诉讼仲裁费用、保全费用、律师费用、维权费用以及其他合理费用。

五、其他约定

1.不放弃权利。除非另有约定，任何一方未能行使或迟延行使其在本协议项下的任何权利，不得被视为其放弃行使该等权利，且任何权利的任何单独或部分行使亦不得妨碍该等权利的进一步行使或其他任何权利的行使。一方在任何时候放弃追究另一方违反本协议任何条款或规定的违约行为，不得被视为该方放弃追究其他各方今后的违约行为，且不得被视为该方放弃其在该等规定项下的权利或其在本协议项下的其他任何权利。

2.协议的变更与修订。本协议如需要补充或修订，协议各方应协商达成一致，并以书面形式作出；非经书面形式的补充和修订，不构成对本协议的有效修改。

六、争议解决

因本协议以及本协议项下附件/补充协议等（如有）引起或有关的任何争议，由协议各方协商解决，也可由有关部门调解。协商或调解不成的，应向甲方所在地有管辖权的人民法院起诉。

七、附则

本协议壹式陆份，甲方肆份，乙方贰份，具有同等法律效力。

本协议未尽事宜，各方应另行协商并签订补充协议。

本协议经各方签名盖章之日起生效。

甲方（章）：

签字：

2026 年 5 月 19 日

乙方（章）：

签字：何岳

2026 年 5 月 19 日