合同编号：

数字秦岭综合监管平台运维项目服务合同

委 托 方（甲 方）： 西安市秦岭生态环境保护管理局（本级）

受 托 方（乙 方）： 数字西安技术运营（集团）有限公司

签订时间： 2026 年 11 月

委托方（甲方）： 西安市秦岭生态环境保护管理局（本级）

联系地址： 西安市长安区关中环线子午段2345号

受托方（乙方）： 数字西安技术运营（集团）有限公司

联系地址： 陕西省西安市经济技术开发区凤城七路正尚国际C座23层

本合同甲方委托乙方就数字秦岭综合监管平台运维项目进行的专项服务，并支付相应的服务报酬。双方经过平等协商，在真实、充分地表达各自意愿的基础上，根据《中华人民共和国民法典》的规定，达成如下协议，并由双方共同恪守。

第一条：甲方委托乙方进行专项服务的内容如下：

1. 软件运维：基础设施维护，数据库及中间件维护，应用系统维护，技术支持与培训，需求收集与功能完善。

2. 硬件运维：前端设备（摄像机、无人机、机巢）日常监测服务，网络设备维护，数据中心设备维护。

3. 安全运维：终端安全，业务应用与服务器主机安全，安全加固，网络安全事件应急响应与演练，网络专线运维，密码安全管理。

4. 其他内容与服务：重点时期（防汛期、防火期及重大活动）值班保障，数据运营支撑服务，数据采买服务（含卫星火点监测数据服务、火险等级预报数据服务等）。

第二条：乙方应按下列要求完成专项服务工作：

1. 服务地点：甲方指定地点

2. 服务周期：自 2026 年 12 月 1 日至 2027 年 11 月 30 日。

3. 服务总体要求：（1）提供日常7x24小时运维服务，主动发现软硬件及网络层面潜在问题、预防战障发生、快速响应并解决系统战障，保障业务连续性；及时发现并修复系统安全漏洞，快速处置网络攻击、数据泄露等安全事件；在重大事件保障时提供应急响应及现场保障，保证各类应用系统正常运行，降低整体管理成本提高应用系统整体服务水平。具体要求详见附件。

（2）服务质量指标：① 监管平台摄像头接入率和在线率不低于90%；② 确保不发生网络安全风险和网络安全事件；③ 保证火情预警的实时性和准确性，不漏报、不误报。

4. 其他要求（如有）：详见招标文件

第三条：甲方向乙方支付专项服务费用及支付方式为：

1. 服务费总额为：人民币 1,999,576.30 元（大写：壹佰玖拾玖万玖仟伍佰柒拾陆元叁角）

2. 服务费由甲方**分期**支付到乙方：

具体支付方式和时间如下：

合同签订、运维人员入场正常开展，乙方向甲方开具合规等额的增值税普通发票，甲方在收到乙方开具的发票后 7 工作日内支付合同总价款的 30%。即人民币（大写）伍拾玖万玖仟捌佰柒拾贰元捌角玖分；￥599872.89 元。

自运维人员入场起项目运维服务半年，甲方在收到乙方开具的发票后 7 工作日内支付合同总价款的 40%，即人民币（大写）柒拾玖万玖仟捌佰叁拾元伍角贰分；￥799830.52 元。

所有服务内容完成并验收合格，甲方在收到乙方开具的发票后 7 工作日内支付合同总价款的 30 %。即人民币（大写）伍拾玖万玖仟捌佰柒拾贰元捌角玖分；￥599872.89 元。

乙方开户银行名称、地址和账号为：

开户银行：西安银行太白北路支行

开户名称：数字西安技术运营（集团）有限公司

账　　号：505011510000018904

第四条：双方确定：

在本合同有效期内，甲方利用乙方提交的专项服务工作成果所完成的新的技术成果，归甲方所有。

第五条：双方权利和义务

（一）甲方权利和义务

1. 甲方在履行合同过程中应遵守法律，并保证乙方免于承担因甲方违反法律而引起的任何责任。

2. 甲方应按合同约定向乙方提供相关资料，以及部署环境，并保证资料和环境的真实、准确、完整。

3. 甲方应按合同约定向乙方及时支付合同价款。

4. 甲方应在乙方提出具备验收条件时，收到乙方书面验收申请后 10 个工作日内及时组织验收。

5. 甲方应配合、协调乙方履行完成合同。

6. 甲方有权对乙方的项目实施进度、成果质量、数据使用情况进行全程监督，对不符合合同要求的事项有权随时提出整改要求；有权要求乙方更换经甲方审核不合格的项目人员及驻场运维人员，乙方应在 3 个工作日内完成人员更换。

7. 甲方应履行合同约定的其他义务。

（二）乙方权利和义务

1. 乙方在履行合同过程中应遵守法律，并保证甲方免于承担因乙方违反法律而引起的任何责任。

2. 乙方应按合同约定实施、完成全部项目，并修补项目中的任何缺陷。

3. 乙方应按甲方要求，签订项目安全协议书，编制与合同内容相关的服务方案。

4. 对全部项目的完备性、稳定性和安全可靠性负责。

5. 乙方应认真执行甲方发出的与合同有关的任何指示，按合同规定的内容和时间完成全部承包工作。

6. 乙方应履行合同约定的其他义务。

第六条：违约责任

（一）甲方违约责任：

1. 如甲方逾期支付合同服务费，则甲方从逾期之日起，按每天逾期付款部分的0.5‰计算并向乙方支付违约金，并且本合同中乙方对甲方的各项服务日期作相应顺延。

2. 如由于甲方原因中途无正当理由单方解除合同而给乙方造成损失的，甲方应承担给乙方造成的直接损失，并向乙方支付已解除部分对应的服务费总值10%的违约金。

3. 由于甲方原因未能按照规定履行自己应负的责任而延误工期，由甲方负责，工期加以顺延，还应赔偿乙方由此造成的实际经济损失。

4. 甲方接到乙方提交的完整且符合要求的验收资料及验收通知后十日内，无特殊原因不能及时进行验收的，视为验收合格；甲方确需延期验收的，应在前述期限内书面通知乙方并说明理由。因甲方无正当理由逾期未组织验收导致工期延误的，且乙方不承担延误工期违约金。

（二）乙方违约责任：

1. 项目质量不符合合同及附件要求规定的，甲方有权立即向乙方提出异议并要求整改，同时有权扣除对应不合格服务部分的服务费；如果乙方拒绝整改或整改后仍不符合合同要求，乙方应承担由此给甲方造成的直接经济损失。

2. 若乙方人员触犯国家法律而被处分时，应及时更换人员。

3. 若乙方未按规定期限完成本项目，每延迟一天（不足一天，按一天统计）扣除逾期交付部分服务费的0.5‰，扣罚不免除乙方完成项目及修补缺陷的义务，扣罚总额不超过逾期交付部分服务费总值的30%。

4. 若乙方未按合同要求提供服务或产品质量不能满足技术要求，且经甲方书面通知后仍未

改正，或整改后仍不符合合同约定标准的，甲方有权单方解除合同，要求乙方退还甲方已支付的未对应合格服务部分的全部款项，并要求乙方支付合同总价款30%的违约金。

5. 乙方提交的项目经验收不合格，乙方应按技术要求返工，返工所产生的直接费用由乙方自行承担。

6. 除法律另有强制性规定外，本合同项下一方对另一方提起的损失赔偿，仅限于有明确证据证明的直接实际损失，对于任何包括但不限于利润损失、声誉损失、数据损失等间接损失，各方都不承担赔偿责任。本合同项下双方应承担的违约金、损失赔偿金额，累计最高均不超过合同总金额的30%。

（三）双方其他违约责任按照《中华人民共和国民法典》的有关条款执行。

第七条：争议的解决方式

1.凡因履行本协议产生的争议，由双方协商解决。协商、调解不成的，应提交至甲方所在地人民法院提起诉讼。

第八条：合同有效期

1.本合同经双方的法定代表人或法定代表人授权委托代理人在合同书上签字并分别加盖本单位的合同专用章后正式生效，自本合同项目款项结清之日起自然终止。

2.合同履行期间，甲、乙双方均不得随意更改或解除合同，本合同的变更及其它未尽事宜，必须经双方共同协商解决。

第九条：本合同一式 肆 份，甲、乙双方各执贰份，具有同等法律效力。

第十条：本合同经双方签字盖章后生效。

甲方（盖章）：西安市秦岭生态环境保护管理局（本级）

地址：西安市长安区关中环线子午段2345号

负责人（签名）：

2026年11月26日

乙方（盖章）：数字西安技术运营（集团）有限公司

地址：陕西省西安市经济技术开发区凤城七路正尚国际C座23层

负责人（签名）：

2026年11月26日

附件：服务要求

一、项目概况

（一）运维对象概况

数字秦岭综合监管平台围绕“五乱治理、森林防火、水质监测”三大业务场景，以“预警分析+综合监管”为核心，采用“1（市级平台）+6（区县子平台）+N（行业系统）”总体架构，构建“空天地网”一体化监测体系。平台2024年7月启动建设、2025年12月完成竣工验收，投资2567万元，面向市级部门和沿山6个区县日常业务使用，用户使用量超过2000人，平均日活跃用户约300人。运维对象包括云平台基础设施、数据库与中间件、业务应用系统、前端感知设备（2055路摄像机、157台无人机、28个机巢）及网络与数据中心设备。

（二）预期目标

提供日常7×24小时运维服务，主动发现软硬件及网络层面潜在问题、预防故障发生、快速响应并解决系统故障，保障业务连续性；及时发现并修复系统安全漏洞，快速处置网络攻击、数据泄露等安全事件；在重大事件保障时提供应急响应及现场保障，保证各类应用系统正常运行，降低整体管理成本，提高应用系统整体服务水平。

二、运维服务内容

本项目运维服务内容分为四大类，投标人须针对全部内容提供完整技术方案：

● 软件运维：基础设施维护、数据库及中间件维护、应用系统维护、技术支持与培训、需求收集与功能完善。

● 硬件运维：前端设备（摄像机、无人机、机巢）日常监测、网络设备维护、数据中心设备维护。

● 安全运维：终端安全、业务应用与服务器主机安全、安全加固、网络安全事件应急响应与演练、网络专线运维、密码安全管理。

● 其他内容与服务：重点时期（防汛期、防火期）值班保障、数据运营支撑服务、数据采买服务。

三、软件运维技术要求

（一）软件运维范围

投标人须对下列软件系统及数据体系提供维护保障：

类型	类别
应用系统维护	应用管理维护、无人机管理、网格管理、运行监测、指挥调度、评估考核、综合态势感知
专题维护	五乱专题、防火专题、水质专题、数字沙盘、网格系统
数据维护	数据库、外部系统接入数据、视频智能解析采集数据、AI算法模型数据、系统数据处理数据、统一权限管理数据、地理信息服务数据及地理信息服务管理平台数据

（二）服务团队配置要求

投标人须配置不少于9名现场驻场人员及2名远程技术支持人员。9名驻场人员须实行7×24小时轮换驻场，其中白天（工作时间）不少于6人现场值班、夜间不少于3人值班，确保系统持续稳定运行；2名远程人员提供技术支撑、后端应用功能完善与系统升级支撑。

（三）详细服务内容及要求

1. 基础设施维护

（1）制定检查标准与方案、检查计划；例行对日志、告警系统、主机/存储/网络系统运行状态（CPU、硬盘、内存、健康度、路由/MAC/ARP/会话表、访问策略）进行检查。

（2）例行输出并通报巡检报告、系统健康性检查报告；对异常内容提供整改方案并实施。

（3）运行监控、定期巡检、专家巡检、调整优化、故障排除、补丁升级、安全加固、资产管理、配置管理。

2.数据库、中间件维护

（1）提供数据库日常检查、性能优化、数据备份与恢复；建立完善备份机制，按日期每月备份一次，并定期验证备份完整性、可用性。

（2）每日主从数据库定时备份，制定异地备份策略；每半年进行一次备份可用性测试及恢复演练。

（3）运行监控、定期巡检、专家巡检、调整优化、故障排除、补丁升级、数据备份恢复、数据迁移、资产与配置管理。

3.应用系统维护

（1）系统日常监测：在服务期内负责对本项目系统运行情况（关键指标项）的日常监测（每日）及定期全面巡检服务。检查的内容包括：1）应用系统的运行状况，是否可访问，各项服务是否运转，系统性能状况，应用系统的日志等。2）各系统间的集成联通状况。3）系统访问日志和访问情况。

（2）定期访问评估：系统在稳定运行期间，定期了解系统状况，对整个系统进行运行质量评估，发现不足，防患于未然。需包含以下内容：系统运行平台常规检查、系统运行质量评估报告、系统运行的建议。

（3）故障处理服务：对偶发性的程序无法正常提供服务情形进行检查处理，比如偶发性用户网络延迟过高，导致流程异常等情形。故障处理遵循“先抢通再抢修”的原则，运维团队需要对以下可能发生的异常情况、系统故障提供排查和修复服务：1）由于新程序漏洞导致的微服务程序和数据库应用之间的连通性阻塞故障处理。需要更新程序的连接池，优化数据库的连接方式以及相关参数。故障修复后对该问题进行持续监控以及优化。2）由于网络策略停用或网络波动导致外部接口无法正常调用。需要排查网络异常的服务器的网络状态，必要时相关接口需迁移至网络健康的运行环境。3）由于程序漏洞导致的系统报错。需要排查问题程序对其故障日志进行错误分析，并且配合开发人员更新程序。应用系统的故障按照故障的定级和处理流程进行处理。通过巡检、监控等发现的应用系统故障，需要及时进行处理。

（4）系统应急演练：常规每半年≥1次（每次≥1.5小时）；重大节假日、系统升级后额外组织1次专项演练（数据恢复专项、网络中断专项等）。

（5）运维知识库及台账：建立运维知识库及运维台账，转运维初期整理蓝图设计、方案、验收报告、操作手册、配置手册、数据字典、部署过程、处理脚本、Bug清单等资料。

4.技术支持和培训

（1）对沿山6区县及市局业务处室提供业务咨询、指导和日常技术支持，保障业务顺利流转。

（2）提供热线支持、文档支持、现场驻场支持、远程协助、用户培训。

5.需求收集和功能完善

系统性能优化支撑、系统升级支撑服务、区县需求收集、系统资源与算法优化（结合业务数据调整算法参数，提升预测分析准确性）。

（四）服务频次

服务内容	服务频次	服务方式	具体要求
服务器资源监控	7×24小时实时监控	人工巡检．	实时监测CPU、内存、磁盘使用率，超阈值（CPU≥80%、内存≥85%、磁盘≤20%）立即告警并处理
操作系统监控	每日1次+每季1次	远程操作+月度驻场优化	对操作系统基础配置和资源使用情况进行统计记录

网络与负载均衡维护	每日巡检+每月测试	远程查看（防火墙日志）+月度驻场测试	每日检查网络带宽使用情况、负载均衡器转发状态，每月测试主备负载均衡切换功能
数据库、中间件运维	每日巡检+按需升级	远程监控+按需驻场升级	每日检查中间件运行状态，每季度根据版本更新情况完成安全补丁升级，升级前需备份配置
核心功能巡检	每日 1 次（9:00-10:00）	驻场人工操作+自动化脚本验证	巡检核心功能，模拟用户操作验证可用性，记录巡检结果
定期访问评估	每季度 1 次+按需优化	远程分析+ 驻场调试	定期分析页面加载慢、接口超时问题，优化前端资源压缩、接口逻辑，将页面加载时间控制在 3 秒内
故障处理	按需处理	远程支撑+ 驻场测试	进行故障修复
功能配置调整	按需处理	远程配置+驻场协助	根据区县需求，调整并测试验证
系统应急演练	定期 1 次/季度+重大节假日等	驻场支持	覆盖驻场服务期间各类系统突发故障（如系统崩溃、网络中断、数据异常、硬件故障等）的应急演练
热线咨询响应	7×24 小时（工作日+节假日）	电话支持	工作日 9:00-17:30 实时响应，非工作时间 2 小时内响应，解答用户操作疑问、申报问题
文档支持	1 次/月+实时更新	文档定期更新	知识库、系统操作文档 F&Q、运维台账等
现场技术支撑	7*24 小时	现场支撑	软件的测试和调整服务，现场技术答疑、客户操作支持
远程协助	7×24 小时（工作日 + 节假日）	电子邮件，短信，微信等	客户疑难答疑
用户培训	每季度 1 次(按需)	驻场培训+线上直播	根据部门需求，开展平台操作培训，培训后提供培训课件与视频回放
系统性能优化支撑服务	每月 1 次+按需优化	驻场调整+远程开发	对用户使用系统过程中遇到的功能问题或性能问题提供优化和完善服务
系统升级支撑服务	每次系统更新升级	驻场调整+远程支撑	提供系统升级支撑
区县需求收集	每月复盘+持续对接	现场收集、电话、电子邮件、短信、即时通讯软件等	主动对接区县及业务处室，收集业务拓展过程中的新需求
系统资源与算法优化	每季度 1 次+按需优化	驻场调整+远程开发	实时监测系统核心资源的使用率，建立资源使用预警机制；对系统中的算法模型进行持续优化，结合业务数据变化和实际应用场景，调整算法参数

（五）软件运维工作产出要求

投标人须按下列频次提交工作产出（各应用系统/专题/数据体系均须执行）：

产出名称	频次
《日常巡检记录》	每日一次
《月度巡检报告》	每月一次
《季度运维报告》	每季度一次
《系统运维总结》	每年一次

《故障记录清单》	每月更新维护
《软件资产清单》	季度更新维护
《数据资产清单》	季度更新维护

四、硬件运维技术要求

（一）服务团队配置要求

本项目拟配置4名工程师提供现场驻场服务，主要运维内容包括前端设备维护、网络设备维护和数据中心维护。4名驻场人员7*24小时轮换驻场，其中白天3人现场值班，1人夜间值班。

（二）详细服务内容及要求

1.前端设备日常监测服务

负责系统内相关硬件设备的日常监测服务，硬件设备包括：前端摄像头、无人机、机巢等，对存在问题故障的设备，属于区县或行业部门建设的反馈区县或行业部门，并及时通知原厂进行问题整改，确保设备在线率和稳定性，保证各项传感数据正常接入系统。纳入管理监测范围的硬件设备主要包含前端2055路监控、157台巡查作业无人机、28个机巢等多类终端设备。持续对设备运行状态及数据传输质量实时排查与动态监管，精准识别设备离线、故障报错、数据中断、性能异常等隐患。

2.网络设备维护

（1）定期现场巡检路由器、交换机、防火墙等关键设备温度、运行灯、端口、内存、风扇等状态；检查网络点到点丢包率、时延。

（2）网络设备配置调整须及时备份并定期提交用户；每季度修改一次设备管理口令；主交换机、防火墙、路由器等重要设备至少每天检查一次，其他设备至少每周一次。

（3）网络割接须遵循规范：提前72小时公告；避让业务高峰（一般0:00-5:00）；“一人操作、一人核查”；重大活动期间不割接。

（4）维护人员对有可能影响业务的网络操作须及时告知，操作后通过网管、现场测试和业务负责人确认业务正常。

3.数据中心设备维护

（1）提供“一点响应”运维制度，7×24小时运行监控，值班严格交接班，禁止关闭可见可闻告警信号。要求值班人员及时响应故障或异常信息，及时进行预处理并记录在案。值班人员对平台定期维护及检查。

（2）落实设备资产台账、设备接入安全（USB/物理端口审批）、备品备件管理、走线规范（三线分离）、存储介质安全管理（异地存放、数据清除）等制度。

服务频次及产出

1.前端设备日常监测服务频次

序号	服务内容	服务配置	服务频次
1	日常巡检	配置2名运维工程师，保证各项前端设备正常运行、监测数据正常接入系统	每日一次，以数据接入情况、在线率和稳定性统计汇报为主。
2	月/季度巡检		每月/季度一次，以月/季度复盘形式。
3	问题反馈通知		无问题时月度总结报告，出现问题及时通知，整改完毕后输出《故障分析整改报告》

2.网络设备维护服务频次

类别	项目	周期
网络设备状态	路由器、局域网交换机状态是否正常	日
	主机设备、存储设备状态是否正常	日
	网络、主机的运行情况	日

	网络（含局域网、出口链路）的业务流量、时延、丢包情况	日
IDC 数据管理	网络数据（含业务数据、网络配置数据）备份	周
	Web 服务器的网页数据备份	周
	KVM 远程控制系统的系统数据及用户数据备份	月
设备物理环境管理	对网络与主机系统物理环境定期检查	周
	定期汇总复盘，对设备物理环境进行专家评估，形成汇总报告	季
	IDC 网络及系统的整体状况	日

3. 数据中心设备维护服务频次

类别	项目	周期
机房环境	灯光、空调等运行情况	日
	人员进出、操作情况	日
	电源系统运行情况	日
机柜	机柜电流记录	月
	机柜配电、端子温度检查	月
其他	设备及机房环境的清洁	周
	主备用设备倒换功能检测	季
	按相关部门的要求，提供运行报表	月

4. 交付成果

成果名称	交付频次	成果形式	具体内容要求
《每日运维日志》	每日 1 次(当日 20:00 前）	电子文档	记录当日设备监控情况、核心功能巡检结果、问题处理情况
《每周运维周报》	每周 1 次（每周一 10:00 前）	电子文档	汇总本周问题处理统计（响应率、解决率）、设备整体情况、下周工作计划
《每月运维月报》	每月 1 次（每月 5 日前）	电子文档+总结汇报	包含月度系统运行报告（可用性、故障次数）、用户服务报告（咨询量、满意度），PPT 用于月度协调会汇报
《季度复盘报告》	每月 1 次（每月 15 日前）	电子文档	本季度日常巡检、周度巡检、设备健康检查、故障处置

故障处置

遵循“业务优先、快速恢复、溯源改进”的处置原则，高效应对设备突发故障。现场出现设备故障时，由运维人员进行快速响应和上报。发现运行故障后，立即启动应急处置流程，先判断故障等级，轻微故障当场处理，复杂故障联系技术人员协同解决，同步记录故障详情。

业务恢复后，组织技术团队开展故障溯源分析，通过查看设备日志、测试硬件性能、排查环境影响因素等方式，明确故障根源。

形成故障处置报告，记录处置过程、根本原因及解决方案，同步更新知识库，优化设备运维预案，避免同类故障重复发生。

一级突发事件：会对关键业务系统产生重大影响的突发事件。故障响应时间为 5 分钟，2 小时内处置完毕。

二级突发事件：部分业务受到影响，核心业务正常运行的突发事件。故障响应时间为 10 分钟，4 小时内处置完毕。

三级突发事件：不影响业务正常运行的突发事件。故障响应时间为 30 分钟，16 小时内处置完毕。

五、安全运维技术要求

（一）终端安全运维

1.每月开展2次办公终端安全防护（病毒查杀与漏洞扫描），形成终端安全查杀记录。

2.运用漏洞扫描工具对操作系统及各类应用软件进行全面扫描，精准识别系统漏洞、组件缺陷等安全隐患，按风险等级排序形成漏洞清单。高危漏洞24小时内完成补丁修复，中低危漏洞3个工作日内修复并复测验证。

（二）业务应用与服务器主机安全运维

1.每月开展1次业务应用和服务器主机安全扫描与渗透测试（自动化+人工），形成安全扫描与渗透测试报告。

2.高危漏洞24小时内修复，中低危3个工作日内修复，修复后须复测，详细记录漏洞情况及修复过程，为系统持续安全提供依据。

（三）安全加固服务

1.对操作系统、数据库、中间件、网络设备、应用系统实施安全加固（最小权限、关闭高危端口、HTTPS加密、访问控制列表、审计日志等）。

2.补丁升级管理：针对操作系统、中间件等，实时关注厂商安全公告，根据漏洞严重等级和业务影响评估补丁优先级，高危漏洞补丁24小时内完成，安装后功能验证并建立台账。

（四）网络安全事件应急响应

建立7×24小时应急响应机制，流程含准备、检测与分析、遏制与隔离、根除与恢复、总结与改进五阶段。

（五）网络安全应急演练

每年开展1次网络安全应急演练，场景覆盖勒索病毒攻击、Web应用入侵、内部数据泄露、DDoS攻击等常见安全威胁，采用桌面推演或实战模拟，结束后形成演练评估报告，针对发现的问题修订应急预案，优化安全策略，并纳入后续培训内容。

（六）网络专线运维

保障秦岭生态环境保护管理局正常访问各级业务系统，每月对各外联单位专线链路稳定性、连通性进行检查，保障应急业务正常访问。

（七）密码安全管理

●依据制度明确密码事件应急处置流程，落实密码产品管理操作规程（验收、监测、维护、变更、故障处置、报废记录）。

●密钥全生命周期管理遵循“分量独立、保密保管、冗余备份”原则，生成、存储、使用、分发、更新、销毁各环节均须审批、双人操作与监督，做好密封保管与交接记录。

六、其他内容及服务技术要求

（一）重点时期值班保障

根据防汛期、防火期及重大活动安排，配合业务处室开展7×24小时值班，调度无人机巡航检查，及时处置火情、防汛及突发事件。须配置不少于3人驻场保障团队（重保期间），确保防汛期、防火期7×24小时值守。

序号	类别	运维产出清单	交付频次
1	重点时期保障服务	《重保期间值守记录》	每次完成重保后交付
2		《问题处理记录》	
3		《资产梳理记录》	
4		《防火防汛值守报告》	
5		《安全保障报告》	
6		《年度复盘报告》	每年1次

（二）数据运营支撑服务

1.数据处理支撑服务：承担基础地理、自然资源、规划管控、专项整治、监测资源等10余个核心数据模块全生命周期维护，建立“入库校验—清洗整合—发布更新”标准化流程（SOP）。

2.告警数据业务处理：建立7×24小时告警数据响应处理机制，实现告警分类分级、关联分析、根因溯源与闭环管理。

3.专项违建数据更新维护：专项违建数据常态化更新维护，按需补充、修正、定期汇总核对。

序号	类别	服务配置	频次
1	数据处理支撑	安排一名专项技术工程师，配合客户进行数据梳理和支撑服务，确保业务正常运转所需的数据支撑	日常更新+定期复盘
2	告警数据业务处理		日常支撑+季度复盘
3	专项违建数据更新维护		按需更新维护+定期汇总

（三）数据采买服务

投标人须通过系统对接方式提供下列数据服务（按月计费，共计12次）：

名称	功能简述	数量/周期
卫星火点监测数据服务	1.提供基于多源卫星融合的5分钟/次高时间分辨率的火点监测数据；GK2A与葵花9号、风云4B卫星观测时间相差5分钟，融合应用实现5分钟/次的火点监测。 2.静止卫星最低时延10分钟，最大时延20分钟。 3.包含5颗静止卫星（FY-4A/B、Himawari-9、GK-2A、GOES-R/S、GF-4）和8颗极轨卫星（风云三号系列、MODIS、NOAA系列等）。 4.依托西电遥感脑算法平台提供行业内最高精度的森林火点监测能力。 人工值班服务： 1.可以根据需求安排专业的火情监测人员进行远程火情监测，完成下垫面判断、异常热源干扰分析云边误判分析等判识，解决卫星监测固有难题，提升监测准确率、减少误报； 2.火情监测人员均统一培训上岗，具有丰富的火情识别经验，可以提升火点辨识准确率，技术应答，火点信息主动推送等； 3.火情值班服务全年无休运行，365*24小时值班，将在重点防火季、重大活动保障期间发挥重要作用。 4.针对漏告警误告警火点专题分析，对重大火情的火势展开分析； 5.实现对各类火点进行分区域，分时段统计分析工作6.输出火点多时次观测、时空分布专题分析与专题图。	12个月
火险等级预报数据服务	基于气象数据、可燃物载量、地表与植被含水量数据、历史火点数据等为基础针对目标区域进行山火风险预测模型计算运行、精细化分析预测，实现空间分辨率：3km*3km，时间分辨率：逐3小时，预测时长：未来72小时。	12个月

七、考核与验收要求

（一）考核指标

为提高运维质量，对运维项目进行运行运维考核，考核得分与年度绩效挂钩，主要分为资料考核和现场考核两个部分内容。

1.资料考核

（1）运行运维计划

序号	检查项	分项分值（扣完为止）	备注
1	所有要求巡检的在管系统功能模块，运行巡检计划	5	检查一年内每月的运行巡检计划，计划零星缺失的每缺失一月计划扣1分；计

	齐全		划连续 3 月缺失的，扣 2.5 分
2	所有要求巡检的在管硬件设备，运行巡检计划齐全	5	检查一年内每月的运行巡检计划，计划零星缺失的每缺失一月计划扣 1 分；计划连续 3 月缺失的，扣 2.5 分

（2）运行运维记录

序号	检查项	分项分值（扣完为止）	备注
1	系统运行巡检记录	5	检查系统一年内每月的运行点检记录，记录零星缺失的每缺一个月记录扣 1 分；记录连续 3 月缺失的，扣 2.5 分
2	硬件设备维护记录	5	检查现场硬件设备一年内每月的运行点检记录，记录零星缺失的每缺一个月记录扣 1 分；记录连续 3 月缺失的，扣 2.5 分
备注	注：以上每项检查不少于 5 个		

（3）安全运维记录

序号	检查项	分项分值（扣完为止）	备注
1	终端安全运维记录	5	检查一年内每月终端安全运维记录，每月 2 次；记录零星缺失的每缺一个月记录扣 1 分；记录连续 3 月缺失的，扣 2.5 分
2	应用与主机安全运维记录	5	检查一年内每月应用与主机安全运维记录，每月 1 次；记录零星缺失的每缺一个月记录扣 1 分；记录连续 3 月缺失的，扣 2.5 分
3	网络安全事件应急预案	5	检查网络安全事件应急预案，若无预案则扣 5 分
4	应急演练记录	5	检查网络安全事件应急演练记录，若无记录则扣 5 分
备注	注：以上每项检查不少于 5 个		

2. 现场考核

（1）人员驻场

序号	检查项	分项分值（扣完为止）	备注
1	驻场人员资质不符合甲方要求，未按规定派驻符合要求的驻场人员提供服务	5	每发现 1 次扣 1 分。
2	驻场人员无故离开值班岗超过 1 小时，小于 1.5 小时	5	每发现 1 次扣 1 分
3	驻场人员更换次数大于等于 2 次	5	每发现 1 次扣 2.5 分
4	驻场人员不服从甲方管理，违反甲方日常办公、机房管理等制度	5	每发现 1 次扣 1 分
5	发生偷盗、失窃等安全事故	5	每发现 1 次扣 2.5 分
6	收到书面投诉	5	每发现 1 次扣 1 分

（2）故障响应

序号	检查项	分项分值	备注

		（扣完为止）	
1	在故障发生后，未在规定时间内提供电话支持及响应	5	每发现 1 次扣 1 分。
2	在故障发生后，故障处理工程师到达现场时间超过 2 小时	5	每发现 1 次扣 1 分
3	在故障发生后，系统回复时间超过规定时间 12 小时	5	每发现 1 次扣 1 分
4	在服务期间，发生操作系统、数据库等系统瘫痪、不可操作、不可管理等事故	5	每发现 1 次扣 2.5 分

（3）安全运维

序号	检查项	分项分值（扣完为止）	备注
1	网络安全事件处置	5	确保重大安全事件（如数据泄露、系统入侵）响应时间≤2 小时，事件闭环率 100%。一年内即时响应。响应时间每超时 1 小时扣 1 分，事件未闭环扣 2.5 分/次，扣完为止。
2	系统网络安全风险被上级单位通报	5	每通报 1 扣 2.5 分，扣完为止。

（二）绩效评价

绩效评级分优秀、合格、不合格三个等级，评价得分高于 90 分（含 90 分）的，绩效评级为“优秀”；得分在 90～60（含 60）分的，绩效评级为“合格”；得分在 60 分以下的，绩效评级为“不合格”。

序号	考评得分	等级
1	≥90	优秀
2	90>得分≥60	合格
3	<60	不合格

根据年度考核总分，将运维服务团队绩效划分为 3 个等级：

优秀：总分≥90 分，运维服务质量优异，超额完成目标；

合格：60 分≤总分＜90 分，运维服务满足基本要求，无重大问题；

不合格：总分＜60 分，运维服务未达要求，存在重大风险（如系统长期宕机、数据泄露等）。

年度考核结果与运维服务费用挂钩，优秀等级按合同金额 100% 结算，并给予内部激励（表彰形式）；合格等级按 100% 结算；不合格等级按 80% 结算，终止下一年度合作资格。