合同编号：9NXCZ2600532EGN00

# 2026年度陕西省自然资源基础网络环境运维项目

## 合同协议书

SNXCZ2600532EGN00

甲方：陕西省自然资源信息中心（陕西省地质资料档案馆）

乙方：陕西公众信息产业有限公司

2026年08月31日

合同编号：8NXOZ2000602EQN00

# 合同协议书

甲方（全称）：陕西省自然资源信息中心（陕西省地质资料档案馆）

乙方（全称）：陕西公众信息产业有限公司

依照《中华人民共和国民法典》及其他有关法律、法规，遵循平等、自愿、公平和诚信的原则，双方就下述项目范围与相关服务事项协商一致，订立本合同。

一、项目概况

1.项目名称：2026年度陕西省自然资源基础网络环境运维项目；

2.项目地点： 采购人指定地点 ；

3.项目内容：依据多部法规及省级相关要求，需保障优化陕西省自然资源信息中心基础网络环境。该网络支撑四级自然资源业务网及多项核心业务，现有多类资源大多已过保，设备老旧，需做好安全防护与运维，保障 “一张网” 及数字政府建设。；

二、组成本合同的文件

1. 协议书；

2. 中标（成交）通知书、响应文件、磋商文件、澄清、补充文件（或委托书）；

3. 相关服务建议书；

4. 附录，即：附表内相关服务的范围和内容；

本合同签订后，双方依法签订的补充协议也是本合同文件的组成部分。

三、合同价款

1.合同金额（大写）：壹佰捌拾肆万玖仟圆整 （￥1849000.00）。

2.合同总价即中标价，不受市场价变化或实际工作量变化的影响。如有合同以外的工作量或技术服务等，双方需签订补充协议。

四、服务

1、服务期限：合同签订之日起一年。

2、服务地点：采购人指定地点

3、服务质量：

3.1 乙方将按照磋商文件要求以及乙方方递交的响应文件、承诺文件来保障服务质量。

3.2 所有服务以及服务配置与响应文件、合同约定的数量、质量及性能，符合磋商文件中提出的要求，所有资源服务均为全新的。

3.3 乙方应当保证所供服务资源的来源渠道正常，并应对所有设备的质量问题负责。

3.4 按照国家相应质量体系要求及项目相关要求，保质、按时、全面地完成项目实施，确保项目服务交付完成。

3.5 在质保期内，如果发现设备的质量、规格、技术指标等存与合中任何一项不符，甲方应立即书面通知乙方，并对产品进行妥善保管，乙方在确认异议无误后应及时进行处理，并追究乙方违约责任。

3.6 采购项目执行内容需要调整时，经甲方同意后，可以对相应的参数指标进行调整，并协商确定价格差额计算方法和负担办法。

五、付款方式：

1、付款条件说明：合同生效，乙方应于甲方每次付款前向甲方开具等额发票，7 工作日内，支付合同额的 60.00%。即人民币（大写）壹佰壹拾万玖仟肆佰圆 （小写）1109400.00，税率为 6%。

2、付款条件说明： 该项目按照约定的验收标准验收合格后，乙方应于甲方每次付款前向甲方开具等额发票， 20 工作日内，支付合同总金额的 40.00%。即人民币（大写）柒拾叁万玖仟陆佰圆（小写）739600.00，税率为 6%。

六、履约验收标准：

1、完成全省线路组网服务，终端杀毒软件授权及升级服务，一体化安全防护系统建设，安全资源池维保升级服务，超融合服务器维保服务，机房资源监管可视化展示服务，办公正版化授权运维服务，防火墙特征库更新升级服务，稳定运行，并有合格的佐证资料。

2、乙方在服务期间应履行好职责，提高服务质量，杜绝推诿扯皮、无故怠工，力争达到服务对象零投诉，做好部、省、市、县四级专网音视频会议系统维保，机房精密空调运维服务，交换机维保，CA 认证平台运维服务，网络安全监测预警和应急处置服务，内部网络系统及安全设备运维服务，应急抢修，故障保障及备品备件储备服务，集成驻场运维服务的内容在服务器的运维工作

3、在服务期间，保证采购人的资产安全。

七、合同争议的解决

合同执行中发生争议的，当事人双方应协商解决，协商达不成一致时，可向甲方所在地人民法院提请诉讼。

八、不可抗力情况下的免责约定

双方约定不可抗力情况指：双方不可预见、不可避免、不可克服的客观情况，但不包括

双方的违约或疏忽。这些事件包括但不限于：战争、严重火灾、洪水、台风、地震等。

九、违约责任：

1.按《中华人民共和国政府采购法》、《中华人民共和国民法典》中的相关条款执行

2.未按合同或磋商文件要求提供产品或供应的产品质量不能满足甲方技术要求，甲方单位有权终止合同，甚至对乙方违约行为进行追究，违约罚款不得超过合同金额的5%。

3.乙方的响应文件为签订正式书面合同书不可分割的部分，乙方应履行相应的责任。

十、保密义务

1、双方同意本合同条款及其附件内之信息乃是秘密，双方有保密之义务，非经对方书面允许，不应将其泄露给任何第三方(根据其适用的法律必须披露的情况除外)。双方同对在合作过程中所获知的对方的企业、技术情报和资料均负有保密义务，任何一方不得将知的对方技术、商业秘密泄漏给第三方(根据其适用的法律必须披露的情况除外)。

2、保密期限原则上为叁年。

3、违反上述规定的直接损失由责任方承担。

十一、合同订立

1. 订立时间：2026年9月24日。

2. 订立地点：西安市莲湖区劳动南路180号。

3. 本合同一式陆份，具有同等法律效力，双方各执贰份，监管部门备案壹份，招标代理机构存档壹份。各方签字盖章后生效，合同执行完毕自动失效。（合同的服务则长期有效）。

甲　方（公章）

单位名称：陕西省自然资源信息中心(陕西省地质资料档案馆)

地　　址：西安市莲湖区劳动南路180号

代 理 人：

帐　　号：610017637000550000492

联系电话：029-87851125

开户银行：建行西安和平门支行

签订日期：2026.9.24

乙　方（公章）

单位名称：陕西公众信息产业有限

地　　址：陕西省西安市长安区

900号秦创原西安科创基金园

代 理 人：

帐　　号：61001902900052506060

联系电话：029-88214949

开户银行：建行陕西省分行营业

签订日期：2026.9.23

合同编号：SNXCZ2600532EGN00

附录 1：

# 分项报价清单

| 序号 | 服务名称 | 服务内容 | 数量 | 单价（元） | 小计（元） | 备注 |
|---|---|---|---|---|---|---|
| 1 | 全省线路组网服务 | 若我公司成功中标该项目，将为采购人提供中国电信股份有限公司陕西分公司数字电路。<br>1、基本要求<br>1.1、网络可用性≥99%，接口实测速率≥接口理论速率×90%，上下行速率差上行速率≥下行速率×99%，年中断次数≤4 次，每次中断时间不大于 4h，排除时间≤4h，故障处理时间响应时间≤30min。<br>★1.2、10 条数字电路（省厅至安康、宝鸡、汉中、商洛、铜川、渭南、榆林、咸阳、延安、杨凌）带宽不低于 200M，服务周期半年；1 条数字电路（省厅至西安）带宽不低于 200M，服务周期一年；1 条数字电路（陕西省不动产登记服务中心到陕西省信息化中心），带宽不低于 50M，服务周期一年；1 条数字电路（省厅至陕西省林业局），带宽不低于 50M，服务周期一年。<br>2、服务要求<br>2.1、合同签订后 7 个工作日内完成线路的开通调试交付工作。<br>2.2、在业务开通后，线路提供商组织人员在三个工作日内上门进行业务交付，具体包括：现场端到端电路测试、现场培训、完成网络测试交付 | 1 项 | 627000.00 | 627000.00 | 无 |

SNXCZ2600532EGN00

| | | | | | |
|---|---|---|---|---|---|
| | | 报告、配合客户完成全网联调等，进行现场培训使客户了解所使用的电路故障申告服务热线及常见故障处理方法等，便于客户确认计费信息。<br>2.3、各项业务开通以后每月进行一次线路检测。一月内或故障申告处理后3日之内，要进行100%回访，及时了解陕西省自然资源厅进网或对故障处理的意见、存在的问题，发现陕西省自然资源厅不满的问题立即组织力量予以解决。要做好回访记录，作为大客户档案资料予以保存。<br>2.4、业务受理：省市两级客户服务部门可以根据采购人的需求，受理采购人的全部业务，并组织调度、调测开通，在承诺的时限内完成采购人的进网工作。对采购人的紧急需求，可采取绿色通道，快速办理。<br>2.5、故障申告：为采购人提供7×24小时故障申告处理和投诉服务。按照“首问负责”的原则，采购人可以就近向当地客户服务热线提出故障申告或投诉，以便获得更加及时的服务。<br>2.6、计费结算：根据采购人需求，本着方便采购人的原则，线路提供商为采购人提供统一的计费结算服务。采购人可以在合同中选择向客户服务部门付费，避免在各地分散交费的烦恼。<br>2.7、技术支持：提供就业务咨询、组网与网络应用、系统集成、网络代维、网络测试、故障诊断等提供全面技术支持，为每个采购人量身定制个 | | | |

SNXCZ2600532EGN00

| | | | | | | |
|---|---|---|---|---|---|---|
| | | 性化的整体解决方案，全面提升客户的价值。<br>2.8、通信保障服务<br>2.8.1 服务目标：保障采购人应用信息网络系统的可靠平稳运行。针对本次省自然资源厅内部网络组网项目，线路提供商将在业务进行期间为省自然资源厅提供完备的信息化建设保障服务。<br>2.8.2 服务内容：将为省自然资源厅内部网络提供信息化建设保障服务，省自然资源厅内部网络在业务进行之前可向运营商提出信息化建设保障需求，采购人应说明服务涉及的项目以及服务时间要求，线路提供商将制定服务保障方案并采取必要的措施保证业务的可靠平稳运行，保障服务措施包括以下几点：<br>2.8.2.1 建立完备的客户档案：将对相应的电路、设备进行特殊标记，以保证其相关维护资料的准确性；建立详细、完备的电路资料档案、网络运行档案以及设备运行参数档案，为保证省自然资源厅内部网络信息网络系统稳定运行提供良好的条件。<br>2.8.2.2 信息网络系统保障：派技术过硬的员工进驻省自然资源厅内部网络有需要的信息网络系统管理机房或现场，协助采购人进行保障工作。<br>2.8.2.3 应急故障处理：为省自然资源厅内部网络制定完善的紧急故障处理流程及应急预案，保证紧急情况下快速进行故障处理，缩短障碍处理 | | | | |

SNXCZ2600532EGN00

| | | | | | | |
|---|---|---|---|---|---|---|
| | | 时间和电路倒接时间。<br>2.8.2.3.1 服务目标：实现“零延时”故障响应。通过多种方式，在最短的时间内响应并解决省自然资源厅内部网络业务运行过程中出现的故障，最大程度的降低网络故障对省自然资源厅内部网络各项业务产生的影响。<br>2.8.2.3.2 服务内容：省自然资源厅内部网络享受运营商大客户的服务。对于省自然资源厅内部网络在业务运行过程中出现的故障，省自然资源厅内部网络可以通过我们的大客户服务获得更为及时的服务响应，提供7×24 的不间断服务。<br>2.8.2.3.3 故障申告方式：省自然资源厅内部网络可选择以下任何一种方式向运营商申告，针对不同等级的网络故障，采用不同的处理方式，并有相应的处理流程提供保证，直到采购人满意为止。全省性故障或复杂、重大故障，省自然资源厅内部网络可以直接拨打绿色通道电话，为省自然资源厅内部网络提供全程联动的故障处理机制，缩短故障历时，并将处理情况反馈给采购人。如果采购人确定故障属于局部地域的本地故障，为方便故障的及时处理，当地的自然资源局可直接向当地服务热线申告。如果采购人认为故障原因和地域无法判明，或与服务热线沟通有困难，可以选择向您的客户经理申告故障，由他代向有关部门申告故障，并全程协调解决，将解决情况告之采购人。上 | | | | |

SNXOZ2600632EGN00

| | | | | | | |
|---|---|---|---|---|---|---|
| | | 述客户服务热线均提供7×24的不间断服务。<br>2.8.2.3.4 故障处理流程：线路提供商承诺为省自然资源厅广域网网络提供7×24小时的不间断服务。在接到省自然资源厅广域网络申告电话后，30分钟内给予故障申告响应回复，同城不大于4小时内解决问题，异地不大于6小时解决问题。 | | | | |
| 2 | 部、省、市、县四级专网音视频会议系统维保 | 服务范围涵盖陕西省自然资源厅三楼大会议室音视频相关设备、十楼二部会议室音视频相关设备。需严格按照设备规范开展运维、维修及升级工作，建立完整的设备全生命周期管理档案，对设备安装配置、日常运行、故障维修、版本升级、优化整改等信息全程记录归档，实现规范化运维管理。<br>我公司对甲方视频会议系统进行全面摸底梳理，形成完整的维保基础资料（包括但不限于系统拓扑图、网络架构图、系统规划表等）。在服务期内，我公司根据实际运维情况及时对运维资料进行更新完善。如果需要对设备进行维护、维修、配置修改、软件升级等，我公司将制定实施方案，充分考虑实施过程中可能存在的风险、降低风险采取的措施、出现问题后的应急措施等。<br>1、巡检服务<br>在服务期内，我公司每季度对甲方视频会议系统相关设备进行巡检、保养，检查系统的接插件线路，发现损坏的设备及时上报，以确保系统的正 | 1项 | 155000.00 | 155000.00 | 服务周期：一年。 |

SNXCZ2600532EGN00

| | | | | | | |
|---|---|---|---|---|---|---|
| | | 常运行。<br>2、日常服务<br>7×24 小时电话支持服务：通过电话支持服务进行响应用户技术支持和故障排除。<br>7×24 小时软件升级支持服务：向客户提供其所购产品的维护性版本或补丁升级版本。<br>7×24（4 小时到达）现场技术支持服务：对于通过电话支持服务和远程接入服务不能解决的设备问题，提供现场支持服务。<br>3. 维保服务<br>针对配套硬件设备损坏、老化、性能衰减等问题，提供专业检测、故障维修、硬件更换及参数调优服务，结合现有会议系统架构开展适配优化，配套部署 1 台视频会议终端设备，解决会议卡顿、断连、延迟、音视频异常等问题，保障各级远程会商高清、稳定、流畅召开。<br>4、培训服务<br>在服务期内，我公司在约定的标准范围内免费提供技术培训服务。<br>5、服务周期：一年。 | | | | |
| 3 | 机房精密空调运维服务 | 机房精密空调是保障机房温度、湿度、空气洁净度恒定的核心设备，是机房内电子设备正常运行的保证，它的正常运行与否，直接关系到机房电子设备的运行状态和使用寿命。因此机房精密空调的日常维护和保养具有极其重要的意义。<br>我公司将针对机房精密空调（两台，分别为世图兹 ASD452A、艾默生 | 1 项 | 35000.00 | 35000.00 | 服务周期：一年 |

SNXCZ2600532EGN00

| | | | | | | |
|---|---|---|---|---|---|---|
| | | DME12M0I2）工作的状况，安排技术人员为用户定期开展空调外机冲洗清洁、过滤网更换、冷媒检测加注；针对高温运行、负荷过高导致的压缩机故障等常见问题，提供故障检测、维修及部件更换服务，全方位保障机房精密空调全年全天候稳定运行。<br>服务周期：一年 | | | | |
| 4 | 防火墙特征库更新升级服务 | 对现有一台防火墙特征库进行升级维保服务。<br>设备核心参数：<br>（1）标准机架式，模块化双冗余交流电源（AC 100－240V，50/60Hz，支持电源故障告警）。<br>（2）标配 10 个 10/100/1000BASE-T 千兆电口、8 个 SFP 千兆光口以及 2 个 SFP+万兆光口。<br>（3）网络层防火墙吞吐量：25Gbps；应用层吞吐量：12Gbps。<br>（4）IPS 入侵防御吞吐量：4.2Gbps；AV 防病毒吞吐量：3.6Gbps<br>（5）全威胁综合吞吐量（FW+IPS+AV）2.8Gbps；最大并发连接数：580 万、HTTP 每秒新建连接：12 万条 / 秒。<br>（6）全面支持 VPN（IPSec/SSL）、入侵防御（IPS）、防病毒（AV）及应用识别与控制，最大隧道数量：4000 条；IPSec 加密吞吐量：1.2Gbps。<br>1、★本次将购买一年特征库（至少包含应用识别特征库、IDP 攻击规则特征库、URL 过滤规则库）定期更新服务，保持防火墙具备监测并防御最新威胁的能力。<br>2、服务周期：一年 | 1 项 | 43000.00 | 43000.00 | 服期 |

SNXCZ2600532EGN00

| | | | | | | |
|---|---|---|---|---|---|---|
| 5 | 交换机维保 | 对现有 3 台交换机提供 1 年维保服务。<br>其中 2 台交换机原有配置：双主控（LST7MPUE0000）；双交换（LST7SFUEX100）；4 电源（PAC3KS54-CE）；24 万光+24 千兆光(LST7X24BX6S0)满配模块；48 千兆电（LST7G48TX5S1）。<br>1 台交换机的原有配置如下：<br>双主控(LST7MPUE0000)；单交换(LST7SFUEX100)；2 电源(PAC3KS54-CE)；48 千兆电(LST7G48TX5S1)。<br>服务周期：一年 | 3 台 | 10000.00 | 30000.00 | |
| 6 | 终端授权及更新服务 | 我公司提供 50 个终端点位安全管理系统授权及更新服务，支持多引擎协同查杀能力，可实现病毒、木马、恶意软件等威胁的检测处置，并具备主动防御功能；支持主流 Windows PC 客户端操作系统，含一年更新维保服务。<br>服务周期：一年 | 1 项 | 5000.00 | 5000.00 | 服务周期：一年 |
| 7 | CA 认证平台运维服务 | 对现有 CA 认证服务提供全年运维保障，包含状态监测、故障处置、证书管理、安全运维、技术支撑等服务内容，保障 CA 认证业务正常、安全、稳定运行，满足日常政务身份认证及安全校验工作需要。<br>服务周期：一年 | 1 项 | 30000.00 | 30000.00 | 服务周期：一年 |
| 8 | 一体化安全防护系统建设 | 我公司提供的安全集中管理系统和入侵检测系统<br>一、安全集中管理系统<br>1、硬件/软件要求： | 1 项 | 430000.00 | 430000.00 | 提供原厂 3 年质保及相关特 |

SNXCZ2600532EGN00

| | | | | | | |
|---|---|---|---|---|---|---|
| | | ★1.1 设备 CPU、操作系统等核心部件满足“中国信息安全测评中心”的《安全可靠测评结果公告》名录；<br>▲1.2 2U 机型，含交流冗余电源模块，≥2*USB 接口，≥1*RJ45 串口，≥1*管理口，≥256G SSD 硬盘、≥4*4T HDD 硬盘，≥1*Raid 卡 LSI-9361-8i，≥4 个千兆电口网卡（2 组 bypass），≥4 个千兆 SFP 插槽，≥2 个接口扩展槽位，≥128G 内存；<br>▲2、性能要求：整机网络层吞吐量≥3Gbps；应用层吞吐量≥500Mbps<br>▲3、功能配置：平台采用软硬件一体的形式；提供运维审计能力，≥50 个运维主机授权数量；提供日志审计能力，≥50 个日志源授权；提供数据库审计能力，纯数据库网络流量≥100Mbps；提供漏洞扫描能力（系统漏洞扫描、Web 扫描、等保配置核查与加固），≥1000 IP 或域名授权；提供主机安全能力，≥30 点国产化客户端授权，≥30 点 Windows 服务器端授权<br>4、平台功能：平台支持的安全功能皆为为同一品牌；支持 web 管理、串口管理、SSH 管理，其中 web 管理使用 B/S 架构，使用 HTTPS 协议；根据三权分立原则，提供系统管理员、安全策略员和系统审计员不同的用户身份验证；支持 CPU 利用率、CPU 温度、内存利用率、硬盘使用率、硬盘 raid 模式等告警阈值配置，超过阈值并产生告警；支持配置向导功能， | | | | 征库升级服务 |

SNXCZ2600632EGN00

| | | | | | | |
|---|---|---|---|---|---|---|
| | | 可针对典型的组件网络配置提供指导以帮助管理员快速部署上线设备，选择可配置的场景包括但不限于：网络安全检测场景、安全运维审计场景、主机安全管理场景、应用安全检测场景；平台提供针对等级保护防护自测评功能，包括等保二级、等保三级所涉及的安全技术、安全管理要求做逐一自评；平台支持在线拓扑绘制，提供拓扑绘制与保存功能。<br>1）运维审计：系统默认自带三权分立用户，系统管理员、运维管理员和审计管理员权限相互制约，缺省用户账号密码遗失后仅能被重置，防止密码泄露不支持找回。支持实时监控通过 SSH、SFTP、RDP、VNC、Telnet、FTP、X11 等协议的操作行为；对监控到的非法操作，可实时手工切断。<br>2）漏洞扫描：漏洞扫描系统的漏洞库数量不少于 420000 条，能够兼容 CVE、CNCVE、CNNVD、CNVD、Bugtraq 等主流标准。具备并支持系统漏洞扫描、web 漏洞、数据库漏洞检查、配置核查和综合分析能力，可输出同时包含漏洞扫描和配置核查结果的报表。支持扫描国产操作系统、应用及软件的安全漏洞，如华为欧拉、open 欧拉、统信、麒麟、bclinux、达梦、南大通用、人大金仓、神通、金蝶、东方通等。<br>3）日志审计：系统支持的数据采集范围包括但不限于网络安全设备、交换设备、路由设备、操作系统、应用系统等。系统支持的数据采集方式包 | | | | |

SNXCZ2800532EGN00

| | | | | | | |
|---|---|---|---|---|---|---|
| | | 括但不限于 SYSLOG、RSYSLOG、SNMP Trap、FTP、JDBC、Net flow、KAFKA、WMI、二进制数据、专用 Agent 等方式采集日志。系统应能够实现范式化日志的枚举值管理，实现对范式化日志字段的灵活翻译。<br>4)数据库审计：主流数据库：Oracle、SQLServer、MySQL、DB2、Sybase、Informix、PostgreSQL、MariaDB、Cache、Teradata、Impala、Greeplum 等国际主流数据库审计。国产化数据库：至少支持 DM、kingbase、OSCAR、Gbase、Highgo、Guass DB、TDSQL-MySQL、TDSQL-PostgreSQL、GoldenDB，TiDB，星环 inceptor 等国产数据库审计。支持旁路镜像部署，Agent 引流部署、混合部署，部署模式可通过界面快速选择与切换。支持高级查询能力，包括不限于：SQL 关键字、结果集关键字查询，提供：与、或、非三种查询依赖条件。<br>5）终端安全：采用 B/S 架构管理，能够进行分组管理、策略制定统一下发、全网终端健康状况监测、可以通过管理端发布统一杀毒、统一漏洞修复命令，支持对终端软件进行管理。支持终端进程黑名单、白名单功能，可设置核心进程必须运行，也可保护核心进程不被结束。对勒索者病毒提供防护机制，并可提供解密工具。<br>▲5、产品资质：国家版权局颁发的《计算机软件著作权登记证书》<br>★6、质保：提供原厂 3 年质保及相关特征库升级服务 | | | | |

SNXCZ2000532EGN00

| | | | | | |
|---|---|---|---|---|---|
| | 二、入侵检测系统<br>1、硬件规格及性能：<br>★1.1 系统应为标准式机架硬件设备，全内置封闭式结构，设备 CPU、操作系统等核心部件满足“中国信息安全测评中心”的《安全可靠测评结果公告》名录。<br>▲1.2 标准机架式硬件，交流双电源，≥2 个扩展槽位，≥2*USB 接口，≥1*RJ45 串口，≥2*千兆电口（1*管理，1*热备），≥128G SSD，≥4T 硬盘，≥6*电口（3 组 Bypass），≥4*千兆光口。<br>▲1.3 网络层吞吐量≥15G，应用层吞吐量≥10G，新建连接数≥21W，最大并发连接数≥400W。<br>2、入侵检测：系统攻击特征库至少有 14000 种，可以针对网络病毒类、蠕虫木马类、扫描探测类、暴力破解类等攻击恶意流量进行检测和阻断。入侵检测支持多种抗逃避检测技术。入侵检测能够提供入侵行为特征的自定义接口，可根据用户需求定制相应的检测规则。系统应能够有效抵御 SQL 注入等多种常见的应用层安全威胁。<br>3、特征升级：厂商应定期升级攻击特征库，遇到重大安全事件，提供即时升级。厂商官方站点需同时提供升级包下载页面，并提供详细的升级事项说明。<br>4、日志归并：系统应具备实时的日志归并功能，可以根据用户需要，按照告警事件的源/目的 IP、事件类型 | | | | |

SNXCZ2600632EGN00

| | | | | | | |
|---|---|---|---|---|---|---|
| | | 等信息，对告警日志执行归并，有效抵御告警风暴。<br>5、用户认证：系统应具备用户身份识别能力，支持基于用户身份进行策略配置、日志记录与查询；支持自动与手动获取用户信息列表并生成组织结构图。<br>6、设备管理：系统应提供标准 snmp trap（V1、V2、V3）和 syslog 接口，可接受第三方管理平台的集中事件管理。<br>▲7、资质要求：提供国家版权局颁发的《计算机软件著作权登记证书》<br>★8、质保：提供原厂 3 年质保及相关特征库升级服务。 | | | | |
| 9 | 安全资源池维保升级服务 | 对现有一套安全资源池提供整体维保及升级服务，具体内容如下：<br>1、为 2 台等保一体机提供一年维保服务，保障设备稳定运行、故障排查及日常技术支撑。<br>2、提供一年云安全管理平台（维保升级服务，具体包括：<br>1 年云安全平台系统升级服务，包含平台系统迭代、BUG 修复、系统补丁更新；<br>13 套安全组件软件升级与规则库更新服务，覆盖对应安全点授权，包含各安全组件的程序版本升级、漏洞补丁修复，以及安全规则库更新。服务周期：自合同签订之日起至 2027 年 12 月 16 日。 | 1 套 | 80000.00 | 80000.00 | 无 |
| 10 | 超融合服务器维保服务 | 对现有 6 台超融合服务器提供专业维保服务，保障设备硬件、系统平台 | 6 台 | 4000.00 | 24000.00 | 服务周期：自合 |

SNXCZ2600532EGN00

| | | | | | | |
|---|---|---|---|---|---|---|
| | | 稳定运行，具体维保时限如下：<br>服务周期：自合同签订之日起至2028年1月21日。 | | | | 同签订之日起至2028年1月21日。 |
| 11 | 机房资源监管可视化展示服务 | 负责自然资源厅机关机房可视化展示系统整体链路适配、信号调试、功能优化与系统融合服务，依托现有机房可视化系统架构，配套部署60寸LED数字电视、视频控制器、内网主机及HDMI高清线缆等相关辅材，完成整套展示链路集成适配、高清传输链路调试、信号参数调优、画面适配优化、系统兼容性调试等一体化集成工作。通过高清传输链路完成前端信号适配与输出对接，保障可视化系统信号传输稳定、画面展示正常、整体功能运转顺畅，实现对自然资源数据中心机房动力环境、设备微监控运行状态、超融合资源系统运行工况的全方位、直观化展示，保障机房运维状态可视、可管、可控。<br>服务周期：一年 | 1项 | 30000.00 | 30000.00 | 服务周期：一年 |
| 12 | 网络安全监测预警和应急处置服务 | 我公司将提供：<br>一、互联网信息系统安全监测<br>依托监测平台对省自然资源信息中心核心业务系统实施7×24小时不间断网络安全监测，持续开展服务可用性巡检、网页防篡改检测，排查页面死链、暗链风险，安全漏洞扫描，保障自然资源业务系统稳定可靠、页面内容合规安全。<br>二、内外网威胁捕捉 | 1项 | 75000.00 | 75000.00 | 服务周期：一年 |

SNXCZ2600632EGN00

| | | | | | | |
|---|---|---|---|---|---|---|
| | | 通过铺设威胁捕捉系统（含硬件），敏锐捕捉各类异常试探行为，弥补传统边界防护短板，有效监测网内东西向隐蔽渗透风险。覆盖典型攻击场景，支持异常登录爆破、端口违规访问、漏洞利用、探测触碰等多类风险识别。即时告警预警，发现威胁第一时间推送告警，缩短应急处置时间，实现从被动防御向主动防御转变。<br>三、安全巡检<br>每月组织现场安全巡检，分析安全设备运行状态、安全告警数据，梳理全网安全态势，跟踪可疑风险线索，快速处置安全突发事件，实施内外网漏洞扫描。<br>四、关键信息基础设施风险评估<br>对省自然资源厅关键信息基础设施执行安全风险评估。针对关键信息基础设施开展威胁脆弱性分析，识别各类安全隐患，分析研判风险并出具风险评估报告。<br>五、数据安全检查<br>对自然资源厅 19 个业务系统开展数据安全专项检查，围绕数据分类分级、访问权限、日志审计、风险隐患开展全面核查，压实数据安全管理各项举措<br>六、资料整理<br>依据网络安全和数据安全法规协助省自然资源信息中心完成制度编制，网络安全文件、事件汇总，各类项目文件汇编。<br>服务周期：一年 | | | | |

SNXCZ2600532EGN00

| | | | | | | |
|---|---|---|---|---|---|---|
| | | 针对国产化内部网络系统及安全设备提供全年驻场运维服务及现场服务，运维服务内容主要包括日常检查、设备巡检、现场保障、故障处理、故障分析、安全检查等，目的是确保该系统的合规化运行。<br>1.日常检查<br>乙方通过每季度一次巡检，检查网络连通性，如有问题远程或现场处理。<br>2.设备巡检<br>运维服务人员对各类设备、网络系统等进行巡检，巡检内容为检查设备硬件运行状态和资源使用状态。主要包括：网络设备检查、应用系统检查、安全设备检查等。<br>3.故障处理<br>协调处理巡检发现及用户反馈的故障及问题，若不属于运维范围内的故障问题应积极协调第三方维护人员处理。<br>4.故障分析<br>运维服务人员进行事件故障采集分析，其主要内容包括：网络层面、系统层面的故障分析。<br>5.安全检查<br>运维服务人员对设备及应用系统进行安全检查，安全检查的内容主要包括：检查设备的用户名口令、防火墙、系统日志并及时修补漏洞，病毒软件的升级等。<br>服务周期：一年 | | | | |
| 13 | 内部网络系统及安全设备运维服务 | | 1项 | 40000.00 | 40000.00 | 服务周期：一年 |
| 14 | 办公正版化授权运维服务 | 提供办公正版软件授权存续及版本更新服务，涵盖文字、表格、演示等全套办公功能，适配日常办公使用需 | 1项 | 20000.00 | 20000.00 | 服务周期：一年 |

SNXCZ2600032EGN00

| | | | | | |
|---|---|---|---|---|---|
| | 求。服务覆盖内网30个电脑终端、外网20个电脑终端，保障终端办公软件合规、稳定、可正常迭代升级。<br>服务周期：一年 | | | | |
| 应急抢修、故障保障及备品备件储备服务 | 建立覆盖全网信息化设备的常态化应急保障与备品备件储备机制，包含光转电模块5块、光模块5块、服务器硬盘（1T大小）3块、服务器内存条（32G大小）3条、转换线1条、六类非屏蔽线缆300米、电话通信线缆100米、运维工具耗材等常用网络物料储备，为现场突发故障提供快速抢修、设备替换、物资支撑服务，确保网络各类业务系统不中断运行。<br>服务周期：一年 | 1项 | 25000.00 | 25000.00 | 服务周期：一年 |
| 集成服务 | 提供项目硬件集成交付、现场部署实施、系统联调测试、全域运维统筹、全程技术支撑及验收移交等一体化驻场运维服务，保障业务稳定运行。<br>服务周期：一年 | 1项 | 50000.00 | 50000.00 | 无 |
| 驻场服务 | 合同签订后，要求供应商根据《运维设备清单》提供驻场工程师，驻场服务如下：<br>1、服务人员应对设备类的整机、CPU、内存、硬盘、网络配置、电源、风扇、操作系统等进行日常巡检、登记，及时跟进各项运行信息；要负责异常或故障的受理、跟踪、解决以及统计分析；负责运行资源的管理，策略备份的制定及执行监控。<br>2、应负责网络规划、部署空间规划、部署位置的规划。<br>3、根据业务访问要掌握网络设备配 | 1项 | 150000.00 | 150000.00 | 服务周期：一年 |

SNXCZ2600532EGN00

| | | | | | | |
|---|---|---|---|---|---|---|
| | | 置、功能、网段划分、网络协议整合网络中的配置数据、表项数据、日志数据、性能数据，监测网络中各个层面的问题和风险。要积极响应网络告警，进行告警、故障应急恢复，通过收集网络中多种故障信息，找到故障相关的线索，实现故障快速准确的分析定位，保障业务持续稳定运行；通过检测范围覆盖工作状态异常、网络容量异常、器件亚健康、业务流量交互异常等范围分析定位，保障业务持续稳定运行。<br>4、应根据业务访问要掌握网络安全设备配置、功能、区域划分、网络安全协议整合网络安全中的配置数据、表项数据、日志数据、性能数据，监测网络安全中各个层面的问题和风险。要积极响应网络安全告警，通过收集网络安全中多种风险信息，找到故障相关的线索，实现故障快速准确的分析定位，保障业务持续稳定运行；通过检测范围覆盖工作状态异常、网络容量异常、器件亚健康、业务流量交互异常等范围分析定位，保障业务持续稳定运行。<br>5、网络安全保障人员要深刻理解从事网络安全保障工作必备的职业素养、服务责任。要理解网络安全保障工作所需基础知识结构，要理解从事网络安全保障工作所需的基本技能。安全运维准备、安全运维实施，参考国家标准或行业标准，对资产进行分类。并响应以下要求：要了解资产分类的技术结构及相互关系、应用方 | | | | |

SNXCZ2000532EGN00

| | | | | | |
|---|---|---|---|---|---|
| | 法，要识别网络安全资产，形成资产清单。对已识别的网络安全资产，掌握网络安全设备配置、功能、区域划分、网络安全协议，梳理、形成网络安全体系资源。整合已识别的网络安全资产配置数据、表项数据、日志数据、性能数据，监测网络安全中各个层面的问题和风险。应对已识别资产的安全管理或技术脆弱性利用适当的工具进行核查，并形成安全管理或技术脆弱性列表。要积极响应网络安全事件，通过收集网络安全事件信息，配合用户找到网络安全事件相关的线索，实现网络安全事件快速准确的分析定位，保障业务安全稳定运行。<br>6、要积极响应持续监控与分析，通过检测范围覆盖状态异常、网络容量异常、业务流量交互异常等范围分析定位，保障业务持续稳定运行。<br>7、要积极响应设备器件、组件亚健康、故障告警，实现器件亚健康、故障快速准确的分析定位，保障业务安全稳定运行。<br>8、要积极响应各项告警，通过收集告警信息，找到告警相关的线索，实现告警快速准确的分析定位，保障业务安全稳定运行。<br>9、要配合用户相关活动，包括但不限于上级检查、安全审计、应急演练、体系评价等。<br>10、每月输出巡检报告一次，特殊情况或者重要阶段需要每天或者每周需要5×8之外的保障运维服务。 | | | | |

SNXCZ2600532EGN00

| | | | | | | |
|---|---|---|---|---|---|---|
| | | 11、故障恢复类：要求 7×24 小时响应支持。支持范围包括产品的功能、配置、安装、调试、客户化以及使用中遇到的各种技术问题的一般性咨询，并随时准备处理各种突发事件。<br>12、故障解决服务：在故障发生后，判断出故障的原因，然后进行有针对性的维修，可缩短故障修复时间，缩短业务中断时间。<br>13、技术服务类：<br>13.1、定期巡检：安排工程师每月进行定期的例行巡检和预防性维护，每周对机房进行硬件运行状态检查，工程师定期对服务范围内的硬件和操作系统、性能进行诊断，分析系统运行情况，查看系统日志，根据结果调整系统参数，使系统始终在良好状态下运行。对可能出现的问题提供科学预测，提供预防整改措施，在授权的情况下必要的预防和补救措施，防患于未然。<br>13.2、常规作业服务：提供硬件、机房环境的常规作业服务，包括设备上下架、安装部署、设备除尘等。<br>13.3、制度梳理：人员入场前针对各系统制定管理计划与管理制度。管理计划分阶段进行优化，在每次定期汇报交流后修改管理计划，形成下一阶段的管理计划，使管理计划与时俱进，更符合系统当前的需求。<br>13.4、资产配置建档服务：提交详细的维护服务档案，内容包括配置、资源使用情况、双方人员信息、维护记录等信息。并根据需方的实际需要， | | | | |

SNXCZ2600532EGN00

| | | | | | | |
|---|---|---|---|---|---|---|
| | | 制定详细的服务支持计划，随时更新硬件系统信息。并根据调研设备的运行记录进行评估。<br>14、专业化服务<br>14.1、服务人员组成有存储、服务器、网络、网络安全、超融合、备份等运维能力，有多个项目经验。<br>14.2、策略、性能优化服务：在用户允许的情况下，对授权操作、策略配置、病毒库、安全规则库升级、配置备份，对数据中心网络进行系统、存储系统、计算资源池、网络安全优化，对以上系统环境进行配置整理，根据整理结果提出优化建议，并实施配置优化。<br>14.3、体系架构规划、资源规划、现网软硬件环境，按需对网络安全做例行巡检、策略优化、规则库升级等工作。<br>14.4、其他服务：确保系统正常运行的其他临时性工作。<br>15、服务人数及要求<br>★15.1 本次响应服务商服务期间至少需提供1名工程师作为一线工程师进行驻场服务，如遇国家法定节假日，要提前安排好值班应急保障人员进行保障服务。<br>15.2 完成日常维护和故障解决，现场工程师解决不了，服务商需提供后台工程师协助解决，半小时响应，1小时到场，保证系统的运行稳定。服务商签订合同的同时，需与采购人签订该项目保密协议。<br>16、考核指标 | | | | |

SNXCZ2600532EGN00

| | | | | | | |
|---|---|---|---|---|---|---|
| | | 16.1、合同期内服务商应确保服务人员稳定。<br>16.2、服务商保证采购人设备（硬件、软件）系统安全、稳定、高效运行。<br>16.3、服务商对于故障处理应有详细的报告记录，包含故障原因、响应时间、解决方案以及合理建议等。<br>16.4、服务商在服务期间应履行好职责，提高服务质量，杜绝推诿扯皮、无故怠工，力争达到服务对象零投诉。<br>16.5、在运维期间，应注重环境卫生，维持现场干净整洁，不得将资产进行外借或转移，保证采购要求及合同约定资产安全。 | | | | |
| 合计 | | | | 1849000.00 元 | / | |

SNXCZ2600532EGN00

合同编号：SNXCZ2600532EGN00

附录2：

# 保 密 协 议

甲方：陕西省自然资源信息中心（陕西省地质资料档案馆）

乙方：陕西公众信息产业有限公司

为进一步加强网络与数据信息安全保障，根据甲、乙方签订的合同相关要求，经甲、乙方协商，双方同意，自愿签订本协议，共同遵守本协议所列条款。

## 一、保密信息

1. 在项目实施过程中所涉及的所有项目文档、系统结构、源代账号及口令、数据库内容、业务核心数据及业务流程、各业务系统相关数据和信息内容，以及其他专有信息等。

2. 甲方设备和系统运行的状态、安全态势等安全监控信息和相关运维信息。

3. 其他甲方未对外披露的资料、信息等内容。

## 二、保密条款

1. 乙方必须遵守国家保密法律法规和规章制度，履行保密义务。

2. 乙方应严格保守甲方的有关保密信息，不以其他任何手段谋取私利，损害甲方利益。未经甲方书面许可，乙方不得在任何时候任何场合以任何名义向第三方（包括乙方所在公司其他与本服务无关人员）泄露甲方保密信息。

3. 凡参与或参与过本项目的乙方工作人员，都应对本项目的数据信息（详见本协议第一条款的内容）予以严格保密，本项目的数据信息只能存储于甲方所指定的介质和设备中，乙方工作人员不得带离指定工作场所，不得以任何方式向任何第三方提供或对外公开；未经甲方许可，不得修改本项目数据信息。

4. 乙方须与本项目相关工作人员签订保密协议，并加强保密教育，严防泄密。

5. 不论本项目合同是否变更、解除、终止，乙方对本项目相关数据信息都有保密义务。

6. 项目实施完毕后，乙方应当按照甲方要求归还或销毁甲方保密信息。

## 三、违约责任

乙方违反本协议书的规定，无论过失与故意，均应立即停止该违约行为，同时甲方有权终止协议并追究乙方的相应责任。

## 四、其他约定事项

1. 本协议未尽事宜按国家有关法律法规执行。

2. 本协议自双方签字并盖章之日起生效，一式陆份，甲乙双方各执叁份，具有同等法律效力。

甲方：陕西省自然资源信息中心（陕西省地质资料档案馆）

（盖章）

法定代表人或

授权委托人：

日期：2026.9.24

乙方：陕西公众信息产业有限公司

（盖章）

法定代表人或

授权委托人：

日期：2026.9.23

SNXCZ2600532EGN00