西安市人力资源和社会保障局信息中心

2026年度数据中心专业维保服务项目

合　同

（项目编号：LZBE2026-1622）

甲　　方：西安市人力资源和社会保障局信息中心

乙　　方：中移系统集成有限公司

鉴 证 方：龙鑫项目管理咨询有限公司

2026年11月

中国　西安

西安市人力资源和社会保障局信息中心

2026年度数据中心专业维保服务项目

合　同

（项目编号：LZBE2026-1622）

甲　　方：西安市人力资源和社会保障局信息中心

乙　　方：中移系统集成有限公司

鉴 证 方：龙寰项目管理咨询有限公司

2026年11月

中国　西安

合　同

依据“西安市人力资源和社会保障局信息中心 2026 年度数据中心专业维保服务项目”（项目编号：LZBE2026-1622），经由龙寰项目管理咨询有限公司组织招标，甲、乙双方协商、确认，为确保该项目的顺利实施，根据《中华人民共和国民法典》等法律法规规定，结合本项目具体情况，签订本合同，共同遵守达成如下条款：

一、 定义

除非本合同另有规定，本合同使用的下列词汇具有如下含义：

项目：西安市人力资源和社会保障局信息中心 2026 年度数据中心专业维保服务项目

最终用户：西安市人力资源和社会保障局信息中心

双方表示：甲方和乙方

合同文件构成：本协议书及附件与下列文件一起构成合同文件：1、招采文件、投标（响应）文件、澄清表（函）；2、中标（成交）通知书；3、合同履行中双方澄清、确认并共同签字的补充文件、技术协议及相关技术报告、项目相关方案及报告等；

二、 项目内容

由乙方为甲方提供服务内容以附件 1 工作任务说明书内容为准。

三、 双方权利和义务

1、甲方

1.1 甲方应为乙方基于本合同所提供的运维服务提供必要的工作环境和便利；

1.2 甲方应向乙方真实、客观的提供附件 1 所涉及全部服务项目所对应资料，以便乙方正常、高效开展本合同项下所需提供的运维服务；

1.3 甲方应按照本合同所约定的付款条件及期限按期足额向乙方支付合同款项。

1.4 甲方有权根据相关项目管理制度对乙方的服务质量、人员考勤等方面进行考核并督促乙方进行整改。

2、乙方

2.1 乙方应按照本合同及附件之约定为甲方提供符合双方约定的运维服务；

2.2 本合同履行过程中，数据中心设备及系统出现故障的，乙方应按照合同及附件要求按时至现场予以处理并排除故障，具体要求以附件 1 为准。

2.3 乙方应建立有服务能力的项目组，具体的项目组成员以投标文件为准，指派 吕振斌 为项目经理，乙方应确保其所指派项目联系人能够高效处理本合同项下的各种情况，如经甲方考核认定联系人不符合合同要求的，甲方有权以书面形式向乙方提交更换申请，乙方审核无误后应予以更换。

2.4 乙方应保证其提供服务不影响甲方的正常办公秩序。

2.5 乙方提供服务应遵守甲方的规章制度及安全管理的相关规定，造成甲方及甲方工作人员财产、人身损害的，应承担赔偿责任。

2.6 甲乙双方不建立任何劳务派遣或类似关系，乙方应向其员工承担用人单位的全部责任，乙方因提供服务造成乙方及乙方人员发生财产、人身损害的，由乙方承担损害赔偿责任，与甲方无关。

2.7 因甲方设备部件损坏需要更换备件、配件的，乙方更换周期不得超过 1 个工作日，并对备件、配件提供自更换之日起至少一年的质保期，且乙方对所有服务设备的全部故障件的维修、更换、配件的运输等均是免费的。所有更换的备件均为与原设备或模块的型号相同，或各项性能规格不低于原有设备或模块的备件。所有因乙方更换的备件问题引发的故障或造成的损失均由乙方承担全部责任。乙方在为故障设备更换备件、配件期间，应自行向甲方提供备机，保证甲方系统及硬件设备的正常运行，不因备件、配件的更换影响甲方系统及设备的运行。

2.8 本合同履行过程中，甲方向乙方及乙方人员提供的信息、材料、技术等知识产权仍归甲方所有；本合同的签订与履行不代表甲方对乙方的知识产权转让和许可，乙方仅可出于为甲方提供服务之目的而使用。乙方在履行本合同过程中产生的所有成果（包括但不限于技术方案、软件代码、数据报告等）的知识产权均归甲方所有。乙方仅享有在本项目中使用该成果的权利，未经甲方书面同意，不得用于其他项目或向第三方披露。

四、 服务期限

运维服务期限为：自合同签订之日起一年。

五、 合同金额及支付

1、合同金额

双方确认，本合同约定提供的服务内容的总金额为¥2871500元（大写：贰佰捌拾柒万壹仟伍佰元整）。具体的费用清单以附件2为准。

由于乙方维护工作不力，甲方委托第三方维护而产生的全部合理费用，由乙方承担。

2、付款条件与时间

2.1 合同签订生效后一个月内，甲方一次性支付给乙方合同总价款的50%，即¥1435750元（大写：壹佰肆拾叁万伍仟柒佰伍拾元整）。

2.2 运维服务期满验收合格后一个月内，支付合同总价的50%，即¥1435750元（大写：壹佰肆拾叁万伍仟柒佰伍拾元整）。

3、付款方式

银行卡转账，付款前乙方须开具等额增值税普通发票。如乙方未能在甲方付款前向甲方开具符合甲方要求的发票，甲方有权拒绝付款，由此造成的损失由乙方承担。

4、每次付款条件满足前，乙方须向甲方开具同等金额的增值税发票，甲方的开票信息如下：

单 位 名 称：西安市人力资源和社会保障局信息中心

开 户 银 行：工行万寿南路支行

账　　号：3700131309201015667

纳税人识别号：126101007578177760

住　所　地：西安

5、因乙方未及时向甲方出具发票或开具的发票不合规导致甲方延迟付款的，甲方不承担逾期付款的违约责任。

6、乙方确保上述账户信息真实准确，若账户信息有误造成乙方未收到款项，损失由乙方自行承担。若乙方更换以上账户信息，应在付款前7日内书面通知甲方，未通知致使乙方未收到费用的，甲方不承担任何责任。

7、双方确认，因甲方财政资金拨款导致的付款迟延甲方不向乙方承担任何违约责任，付款时间相应顺延。

六、 变更

1、乙方需要保证项目主要人员的稳定性，项目实施中如有人员变动，在征求甲方同意后，需提前 10 个工作日以书面形式通知甲方。主要人员至少包括：乙方的项目领导小组成员、项目经理，技术（业务）骨干。因未及时通知而造成的项目实施延误的直接损失，由乙方承担。

2、签约方确认，在履行合同过程中对于具体内容需要变更的，由签约各方另行协商并书面约定，作为本合同的变更文本。

七、 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，非经对方的书面允许，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）。

2、双方同意对在服务期内，运维过程中产生的文档（包括维护巡检文档、性能评估及技术方案）均负有保密义务，任何一方不得将秘密泄漏给第三方（根据其适用的法律必须披露的情况除外）。

3、双方同意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，任何一方不得将获知的对方技术、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）。

4、在乙方相关人员知悉该保密信息前，应向其说明保密信息的保密性及其应承担的义务，保证上述人员同意接受本条款的约束，乙方同时应对上述人员的保密行为进行有效的监督管理。乙方如发现甲方向其披露的相关保密信息泄露，应采取有效措施防止泄密范围进一步扩大，并及时告知甲方。

5、合同履行期间双方均应遵守合同规定的保密义务。违反上述规定的直接损失由责任方承担。

6、双方具体的保密义务可参见附件 3 保密协议，本合同解除或终止后，双方仍需遵守本条及保密协议约定的保密义务。

八、 违约责任

本合同任何一方不履行合同或履行合同义务不符合约定条件，即构成违约，另一方有权要求违约方支付合同总价 10%的违约金或者采取补救措施，违约金不足以弥补损失的，有权要求赔偿损失。

1、合同中未约定的，按《民法典》中的相关条款执行。

2、未按合同要求提供服务或服务质量不能满足合同要求，甲方应当将乙方违约的情况以及拟采取的措施报政府采购监管部门，根据政府采购监管部门的处理意见，甲方有权依据《民法典》有关条款及合同约定解除合同，乙方应向甲方支付合同总价款10%的违约金。同时，政府采购监管部门有权依据《政府采购法》及相关法律法规对乙方的违法行为进行相应的处罚。

3、甲方无正当理由解除合同的，需向乙方偿付本合同总价10%的违约金。

4、若乙方违反合同约定的保密义务的，应承担由此给甲方及第三人造成的损失，并尽最大可能防止泄漏的扩散或损失的加重，且乙方应向甲方支付合同总价款10%的违约金。

5、在合同履行中，如因乙方原因给甲方造成损失的，乙方应当承担甲方损失的赔偿责任。

6、如发生违约事件，守约方要求违约方支付违约金时，以书面方式通知违约方，内容包括违约事件、违约金、支付时间和方式等；违约方在收到上述通知后，应于5个工作日内答复对方，并支付违约金。如双方不能就此达成一致意见，将按照本合同所规定的争议解决条款解决双方的纠纷。

7、在运维服务期内，乙方未履行合同约定的服务内容、延迟向甲方提供服务或者未在约定的时间内完成服务内容的，乙方应支付违约金。发生一级、二级故障乙方未在约定时间内响应或恢复业务，每发生一次支付合同总金额5%的违约金，发生三级至四级故障的乙方未在约定时间内响应或恢复业务的，每发生一次支付合同总金额1%的违约金。如有上述扣款情况发生，甲方有权直接从未付给乙方的款项中抵扣（故障内容见附件 1）。

8、甲方有权在支付剩余款项时直接扣除上述违约金，合同期间乙方发生上述情形大于五次的（包含本数），甲方有权单方解除合同，并向甲方支付合同总金额10%的违约金，并赔偿由此给甲方造成的损失。

9、乙方违反合同约定进行转包或分包的，甲方有权解除合同，并要求乙方承担合同总价款20%的违约金，若违约金不足以弥补损失的，还应当承担赔偿损失的责任。

10、乙方提供的服务未达到合同约定的标准或相关法律法规、行业要求标准，甲方有权要求乙方限期整改，整改所发生的费用由乙方自行承担。若因乙方拒绝整改或

整改后仍不符合甲方要求的，乙方应按合同价款 20%向甲方支付违约金。

11、合同履行期间，因乙方原因导致甲方设备系统损坏的，乙方应予以修复，无法修复的，乙方应向甲方赔偿设备损坏的损失；如因前述情形导致甲方设备、系统或数据永久损毁灭失的，乙方还应向支付合同价款 10%的违约金。

12、如果甲方因在乙方授权范围内使用乙方提供的软件、文件资料等，而遭到的第三方就侵犯专利、商标、工业设计或其他知识产权而提出的索赔和诉讼，由乙方承担全部法律后果，如因该等情形导致甲方损失的，乙方应给予甲方全额赔偿。

13、甲方在服务期截止前一个月内就乙方的服务质量、人员考勤管理等方面进行考核考核分数在未达到 90 分的，扣除合同金额的 1%，未达到 80 分的，扣除合同金额的 3%，未达到 60 分的，扣除合同金额的 5%，考核标准见附件 4。

14、任何一方对自然灾害及其他不可抗力原因造成的迟延履行、不完全履行或不履行义务均不应视为违约。

九、 验收

1、服务资料交付载体：乙方向甲方交付电子文档 U 盘一套，资料包括但不限于服务过程中涉及到的《驻场运维保障服务技术方案》、巡检表、故障排查表、运行监测表、重大会议保障记录、设备运行状况月报表、驻场服务工作情况报告等甲方要求提供的资料。

2、交付时间：以项目验收确认时间为准。

3、地点：甲方指定地点。

4、验收方式：

4.1 项目服务期满乙方提出验收申请后，由甲方组织验收。采用现场验收的模式（必要时请有关专家），对项目服务内容进行验收，由甲、乙双方盖章确认。验收不合格的，乙方应当在 5 个工作日内消除造成验收不合格的原因，并承担由此引发的一切费用。否则甲方有权解除合同，乙方应支付合同总金额 10% 的违约金，给甲方造成损失的，应当赔偿甲方损失。验收合格后，填写政府采购履约验收单（一式五份） 作为对服务的最终认可。

4.2 乙方向甲方提交项目实施过程中的所有资料。以便甲方日后管理和维护。

5、验收依据：

5.1 公开招标文件、投标文件、澄清表（函）；

5.2 本合同及附件文本；

5.3 国家相应的标准、规范。

十、 不可抗力

在本合同执行的过程中，由于发生战争、洪水、台风、地震、疫症或其他人力不能控制等不可抗力事件，致使本合同的任何一方无法履行本合同规定的义务，遭受不可抗力的一方不承担违约责任。遭受不可抗力的一方需及时通知对方，应在不可抗力事件发生的 30 日内，向本合同对方出具有关权威部门的证明。

十一、 合同中止

1、如果乙方有下列情形之一的，甲方可以中止履行合同：

1.1 经营状况严重恶化；

1.2 转移财产、抽逃资金，以逃避债务或丧失商业信誉；

1.3 丧失与实现本合同目的密切相关的经营资格；

1.4 有丧失或者可能丧失履行合同能力的其他情形。

2、如果甲方有下列情形之一的，乙方可以中止履行合同：

2.1 无正当理由迟延付款超三个月；

2.2 达到阶段完成标准后，无正当原因无法在一个月内组织阶段性验收；

3、合同中止时，应根据合同实际执行情况，一方需向另一方支付因履行合同的相关合理费用（包括但不限于服务费用、货款等）。

十二、 合同解除

1、经双方书面协商一致，可提前解除合同，双方不负违约责任。

2、乙方存在以下情形之一的，甲方有权单方解除合同，另行委托第三方服务。乙方应返还已支付合同款项，并支付本合同约定的违约金，给甲方造成损失的，还须赔偿甲方因此遭受的所有损失：

2.1 乙方提供的服务未能达到本合同约定或乙方承诺的两次以上的；

2.2 乙方未经甲方书面同意，擅自将合同内容转委托的；

2.3 乙方存在其他违约行为，经甲方书面通知一次后，仍违约的；

2.4 乙方存在严重违法行为的；

2.5 乙方被吊销营业执照的；

2.6 乙方私自复制或向任何第三方泄露甲方提供的任何文件、信息的；

2.7 其他造成甲方重大损失的。

十三、 通知

本合同规定之通知应以书面方式送达至另一方。任何一方变更通知方式，应于变更后三日内书面通知对方，未予通知的，以变更前的通知方式送达视为有效送达。

十四、 管辖及争议的解决

本合同的解释、效力、履行及其他事宜，均受中华人民共和国法律、法规的管辖。如双方因履行本合同发生任何争议，应首先协商解决；协商不成，任何一方均可向甲方所在地法院起诉。

十五、 本合同效力

本合同条款及其附件和本项目的招投标文件构成双方的全部约定。双方以书面方式对本合同条款及附件进行修改和补充，经双方协商同意后的该书面修改及补充与本合同具有同等法律效力。

如本合同有任何条款被司法机关视为无效、被撤销、不合法或不可执行，不影响本合同其他条款的效力。

十六、 送达条款

本合同联系方式和联系信息适用于双方往来联系、书面文件送达及争议解决时法律文书送达。因联系方式和联系信息错误而无法直接送达的自交邮后第 7 日视为送达。双方指定联系地址与联系方式如下：

甲方联系人：武余余 ，联系电话： 029-82282994 ，联系地址： 陕西省西安市雁塔区建工路 28A 社保大厦

乙方联系人：刘超，联系电话：13468842575，联系地址：陕西省西安市雁塔区唐延路 11 号，邮编：710000，电子邮箱：13468842575@139.com。

十七、 其他

本合同自双方的法定代表人签字（盖章）或委托代理人签字并加盖各自公章之日起生效。双方的法定代表人亦可以授权书授权其他人事签署本合同。

投标文件及澄清内容为本合同不可分割的组成部分。

本合同一式陆份，甲方执肆份，乙方执壹份，采购代理机构执壹份。签字盖章后生效，合同执行完毕自动失效。

（以下无正文）

甲方	乙方	鉴证方
西安市人力资源和社会保障局信息中心（公章）	中移系统集成有限公司（公章）	龙寰项目管理咨询有限公司（公章）
地址：西安市雁塔区建工路28号	地址：石家庄市青园街220号	地址：西安市高新区太白南路181号A座
邮编：710043	邮编：050021	邮编：
法定代表人：	法定代表人：王昀	法定代表人：
授权代理人：	授权代理人：刘超	授权代表：
电话：029-82282994	电话：80998630	电话：029-88228899-653
传真：029-82282994	传真：/	传真：029-88228899-653
	开户银行：招商银行股份有限公司北京分行营业部	开户银行：
	账号：8888015100002818	
日期：2026年11月27日	日期：2026年11月27日	日期：2026年11月27日

附件 1：工作任务说明书

工作任务说明书

一、 项目概况

本项目为西安市人社局数据中心提供全栈运维支撑，覆盖硬件、网络安全、数据防护等全维度服务，保障全市人社业务 7×24 小时稳定运行。

二、 采购内容

（一）招标要求

服务期限：合同签订之日起一年

服务地点：采购人指定地点，提供驻场服务。

考核（验收）标准和方法：1.服务专业性：参照 GB/T 25000.51 和 GB/T 16260.1-2006、《西安市信息化项目管理办法（暂行）》（市政办发〔2024〕2 号）、《西安市信息化项目验收实施细则（试行）》（市数发〔2025〕12 号）、等级保护三级有关要求执行， 按照合同要求完成服务内容，验收资料齐全、合理； 2.响应及时性：遵守合同约定的服务响应要求； 3.安全性：发生运维故障恢复时间满足合同要求。

（二）技术要求

序号	参数性质	技术参数与性能指标
1		**一、项目概况和建设目标** 本项目服务对象为西安市人力资源和社会保障局数据中心机房，该机房是承载全市社保经办、就业服务、人事人才、劳动关系等民生类核心业务的专属数据枢纽，直接支撑全市各级人社办事窗口、线上公共服务平台的 7×24 小时业务运转，服务覆盖百万参保群众和各类用工单位。本次采购将为该机房提供全栈技术服务支撑，具体覆盖硬件设备的常态化监控与运维、网络及安全设备的全生命周期管理、安全防护与数据备份策略的落地执行、系统与应用程序的版本迭代和日常维护、全场景故障快速排查与闭环解决、性能持续调优以及稳定运行环境的全方位保障。 **二、服务内容** **2.1 设备维护服务保障** 设备维护服务保障围绕数据中心全场景开展工作，覆盖日常巡检、风险防控等基础运维，响应设备操作、故障处置与设施变更需求，完成性能调优、运行评估，配套完整硬件运维清单，保障数据中心设备长期稳定可靠运行。 **1. 数据中心日常维护** （1）数据中心日常巡检。一是运维平台实时监控。动环、网管、网页系统实时监控与告警处理。通过动环、网管、网页监

		测等平台开展 7×24 小时持续运维监测，实时掌握机房环境、网络流量与带宽、设备运行状态、业务访问性能等关键指标，自动识别异常并快速处置，实现可视化、全覆盖、可追溯的运维保障，提升整体运行可靠性。二是设备告警实时监控。监控硬件、网络、系统、数据库、中间件告警并处置。对数据中心服务器、存储、网络、操作系统、数据库、中间件等对象开展 7×24 小时不间断告警监控，实时捕获硬件故障、链路中断、系统过载、数据库异常、中间件不可用等事件，按等级快速响应、研判、处置、上报并闭环管理，保障业务系统连续稳定运行，降低故障影响范围与时长。三是设备健康日常巡检。机房环境、服务器、存储、网络、数据库、虚拟化设备状态巡检。每日对机房环境、物理服务器、存储设备、网络设备、数据库、中间件及虚拟化平台开展全面健康巡检，检查运行状态、环境参数、连接情况、资源占用与设备健康度，及时发现隐患、记录台账、上报处理，确保硬件与系统平稳运行，为业务持续提供可靠支撑。四是数据中心值班值守。非工作时间段对设备、温湿度、电力、门禁、监控提供专人驻场夜班值守，对机房硬件设备运行状态、温湿度、UPS 及供电系统、门禁安防等进行不间断监控，及时处置夜间告警、环境异常、电力波动与突发状况，严格执行值班与交接班制度，保障数据中心夜间运行安全、稳定、可控。 （2）数据中心风险预防。一是每周设备巡检。每周对数据中心硬件设备、网络链路、系统运行状态、数据库、虚拟化平台、机房基础环境开展全面检查，及时发现硬件隐患、链路异常、性能瓶颈、环境风险等问题，形成标准化巡检记录并闭环整改，保障硬件与基础环境稳定可靠运行。二是月度性能分析。每月对服务器、存储、数据库、网络、安全、虚拟资源、备份系统的负载情况与运行趋势进行全面分析，采集 CPU、内存、磁盘、网络、数据库、虚拟化等关键指标，识别资源瓶颈、评估系统承载能力，形成月度性能分析报告，为系统优化、容量规划、隐患预防提供数据支撑。三是季度深度健康检查。每季度对硬件、操作系统、网络、安全、虚拟化架构开展全面深度健康检查，覆盖设备健康、系统配置、网络架构、安全策略、虚拟化平台等内容，同步核查备份系统执行有效性，输出全面检查报告与备份巡检报告，全面排查潜在风险，保障系统稳定、安全、可持续承载业务。四是备份有效性验证。通过合理备份技术对计算资源、数据库、文件等进行定期备份，包含本地和异地备份。本地依托备份一体机，按增量+全量策略；同城政务机房托管灾备设备，实现核心库近零 RPO 实时同步；离线采用 NAS 介质，每季度归档核心数据。每月对本地及异地备份系统进行全面核查，验证全量备份与增量备份执行状态、备份数据完整性、存储有效性及可恢复性，通过核对与抽样恢复测试，确保备份数据安全可靠，故障发生时可快速恢复业务系统。五是核心资产核查。每季度对数据中心全部 IT 软硬件资产开展全面盘点、配置核对、信息更新与台账维护，覆盖硬件设备、操作系统、数据库、中间件、虚拟化软件等资产，完

		成登记分类、信息更新、下架入库、配置审查留档，确保账实相符、状态准确、管理合规。 （3）数据中心基础运维。一是系统补丁更新。依据运维管理要求与官方安全公告，对数据中心内操作系统、中间件、数据库、虚拟化平台开展补丁升级、漏洞修复及版本更新工作，通过规范的升级流程保障系统组件安全稳定，消除已知漏洞风险，保障硬件与软件平台平稳可靠运行。二是配置文件备份。对数据中心内系统、网络设备、虚拟化平台的关键运行配置进行定期备份，确保配置信息完整可查、快速恢复，在设备故障、配置变更失误、系统异常时能够快速恢复配置，保障业务持续稳定运行。三是日志归档清理。按照运维策略与存储管理要求，对数据库、网络设备、安全设备产生的系统日志、操作日志、安全日志按周期进行归档存储与过期清理，释放设备存储空间，保障系统运行效率，同时满足日志留存与审计要求。四是机房常规维护。每季度对机房环境及硬件设施开展标准化维护工作，包括机柜标签更新、设备上架下架、弱电线缆规整梳理、设备清洁除尘等，保持机房布局规范、标识清晰、布线整齐、环境洁净，提升硬件设备运行可靠性。五是专线检查。为保障区县、医院、银行外联区正常访问人社各级业务系统，确保专线链路访问和安全等问题及时处理。每月对区县、医院、银行等外联单位专线进行连通性、稳定性、链路状态检查，测试专线通断、时延、丢包、抖动等指标，及时发现线路异常并处置，保障人社业务外联访问稳定通畅。六是办公区域网络维护。对人社大厦各楼层出口网络进行维护。七是运维文档输出。严格按照运维管理要求与频次，按期、规范、完整输出各类巡检、监测、运行、资产、演练、服务报告，实现运维工作标准化、可追溯、可审计。 **2. 数据中心服务响应** （1）设备运行例行操作。一是设备资源分配。根据业务系统运行需要，提供虚拟机 CPU、内存、磁盘资源调整及服务器、存储资源分配服务，按规范完成配置下发、可用性验证，保障资源合理供给、平台稳定运行，符合运维管理规范与容量规划要求，确保资源分配可追溯、可核查。二是数据库资源分配。根据业务系统运行需要，提供数据库 CPU、内存、存储空间、连接数等资源的调整与配额分配服务，按规范完成参数下发、可用性验证，保障数据库资源合理供给、运行稳定，符合运维管理规范与容量规划要求，确保资源分配全流程可追溯、可核查。三是网络资源管理。依据业务访问、系统互通需求，在网络与安全设备上完成端口策略配置、开通与放通服务，确保端口开放合规、访问可控、业务通信正常，不引入安全风险，同时做好配置记录与台账管理。四是资产配置调整。提供系统、网络、数据库、虚拟化平台配置信息查询、核对与导出服务，确保配置信息准确、可查、可追溯，协助完成配置核查、故障定位与信息确认工作，满足运维管理与合规要求。五是设备移机管理。为设备迁移提供全流程技术支撑，包括设备拆卸、运输防护、上架安装、加电调试，确保移机过程

		安全无损坏、移机后设备正常上线运行，衔接后续运维工作。对新购设备协助进行设备上架、网络调试等工作，确保设备运行稳定。六是专业维保服务。保证机房内网络安全、存储、负载均衡等设备，由持有专业认证资质的工程师团队提供专属技术保障。七是运维工单响应。承接服务台下发的日常运维工单，完成虚拟机发布、网络配置、数据库配置等相关服务，确保工单及时受理、规范处置、按时闭环，提升运维服务效率与满意度。 （2）数据中心故障处置。一是设备故障硬件更换。对服务器、存储、网络设备出现的硬件故障进行诊断、部件修复与更换，快速恢复硬件运行能力，保障业务系统稳定运行，减少故障对业务的影响，做好故障记录与台账更新。二是数据库故障硬件更换。对承载数据库的服务器、存储等硬件设备出现的硬件故障进行精准诊断、部件修复与更换，快速恢复硬件运行能力，保障数据库服务稳定运行，最大程度降低故障对上层业务的影响，同步做好故障记录与台账更新。三是系统异常恢复。对操作系统、数据库、中间件、虚拟机出现的异常宕机、服务中断、报错等问题进行排查、修复与恢复，保障系统快速恢复可用、业务不中断，做好故障分析与记录。四是性能问题排查。针对系统负载高、业务响应慢、I/O 异常等性能问题开展指标采集、瓶颈定位与优化处理，提升系统运行效率，保障业务流畅运行，形成性能排查与优化记录。五是网络故障修复。针对系统负载高、业务响应慢、I/O 异常等性能问题开展指标采集、瓶颈定位与优化处理，提升系统运行效率，保障业务流畅运行，形成性能排查与优化记录。 以上故障出现重大问题，按照《西安市人力资源和社会保障局信息中心网络与信息安全突发事件应急处置预案》要求，启动突发事件应急预案。一是重大突发事件处置。对硬件宕机、网络中断、数据异常、机房突发事件等重大突发事件进行紧急处置、快速恢复，最大限度降低业务影响，保障业务连续性与数据安全。二是 7×24 小时应急响应。提供全年 7×24 小时应急响应服务，接收故障与突发事件上报，快速协同处置、恢复业务，保障业务不间断运行，提升运维服务响应效率与可靠性。三是应急演练。按计划开展四次系统故障、网络故障、数据恢复等应急演练，检验应急预案有效性、人员处置能力，优化应急处置流程，提前规避突发风险，保障业务连续性。 （3）数据中心设施变更。一是设备上下架。完成设备上架、安装、调试、入网部署，确保设备规范上线、纳入运维管理体系，满足业务运行需求，保障设备运行稳定、合规。二是网络策略调整。根据业务运行、合规及架构优化需求，对数据中心网络设备、安全设备、无线设备、负载均衡设备及日志审计相关策略进行优化配置与变更实施，保障网络传输高效、策略合规、访问可控、运行稳定。三是应用系统迁移。在服务期内，如有数据迁移、服务迁移、存储共享等需求时，应在充分了解实际的应用和系统的情况下，为系统和数据迁移，资源共享提供完善的方案，高效的完成业务系统的迁移部署、变更、应用验证和测试等，保证在迁

		移或共享过程中关键业务和数据可以持续运行。四是虚拟化资源变更。根据业务负载变化，对虚拟化资源进行调整，包括虚拟机扩容、缩容、合并、闲置资源回收，提升资源利用率，保障虚拟化平台运行稳定，满足业务动态需求。五是数据库专项变更。根据业务迭代、性能优化及等保合规要求，完成数据库版本升级、参数调整、分片扩容、主从架构切换、账号权限变更等配置操作，全流程执行变更前风险评审、变更中分步操作、变更后业务校验，确保变更过程无数据损坏、业务无中断，适配业务发展的性能与架构需求。六是备份体系专项变更。结合数据安全防护与容灾合规要求，完成备份策略全维度调整，包括备份周期修改、保留时长配置、存储路径迁移、备份介质轮换、异地容灾备份链路变更，同步配套变更后的备份有效性校验与恢复性测试，保障备份机制持续满足数据不丢失、故障可快速恢复的核心要求。七是应用服务变更。对网络、安全、数据库相关的应用服务进行配置变更与上线，确保变更合规、风险可控、业务稳定，满足业务发展与安全合规需求。 **3. 数据中心性能调优** 一是服务器资源优化。针对物理服务器运行状态开展全面负载分析与系统参数调优，提升硬件资源利用率与系统运行稳定性，保障服务器高效、安全、持续承载业务。二是数据库调优。对数据库运行状态、存储结构、性能瓶颈进行深度优化，包括表空间管理、索引优化、存储压缩、高水位线回收等，提升数据库查询效率、存储利用率与整体运行性能。三是虚拟资源优化。对虚拟化平台资源分配与使用情况进行分析，优化虚拟机 CPU、内存、磁盘配置，回收闲置资源，提升虚拟化平台资源利用率与运行稳定性。四是资源调度与负载均衡优化。基于数据中心全局业务负载画像，动态调整跨服务器、跨集群的资源调度策略，优化负载均衡设备的分发算法、会话保持规则与健康检查机制，消除局部资源热点，实现业务请求的智能均匀分发，保障高并发场景下全链路负载均衡无单点瓶颈。五是存储优化。对集中式存储、分布式存储集群的 IO 路径、块存储分层策略、冗余校验机制进行梳理调优，清理存储碎片、调整冷热数据自动迁移规则，优化存储读写响应时延与 IOPS 性能，同时匹配存储容量动态预警机制，避免存储资源过载影响业务运行。六是网络架构优化。对数据中心网络架构、流量流向、带宽使用、链路冗余策略进行梳理与优化，提升网络可靠性、安全性与传输效率，保障业务访问流畅。七是物理架构优化。对机房物理布局、硬件设备连接关系、机柜规划、设备摆放位置进行梳理与优化，提升机房空间利用率、设备散热效果与运维便捷性。八是备份策略优化。完善数据备份体系，优化全量+增量备份、本地+同城+离线备份策略，确保备份高效、完整、可恢复，提升数据安全与业务连续性保障能力。九是运维与管理优化。围绕日常运维全流程优化管理机制，完善性能基准线动态更新规则、变更操作前置校验流程、日常巡检自动化脚本配置，统一各类设备的性能监控指标口径，建立性能问

题快速闭环响应机制，实现日常管理变更的标准化、可追溯，从管理层面持续巩固性能调优成果，避免性能问题反复出现。

4. 数据中心运行评估

一是资产性能评估。对数据中心全量 IT 资产开展性能维度的全面排查，覆盖服务器、存储设备、网络设备等硬件，以及操作系统、配套应用程序等软件，同步梳理相关配件的运行状态。逐台/逐系统采集实时运行数据，记录型号、序列号、配置参数、网络地址等基础信息，结合历史运行数据做性能基准对标，每季度完成一次全量性能数据更新，形成动态更新的性能台账，精准掌握每台设备的性能负载、健康度情况，提前识别硬件老化、性能冗余不足等潜在风险。二是数据库专项运行评估。针对所有在线数据库开展全维度专项评估，覆盖数据库运行稳定性、查询响应效率、存储资源占用、主从同步状态、备份有效性、账号权限合规性等核心维度，梳理当前存在的慢查询、表空间溢出、索引失效等性能隐患，评估数据库架构对当前业务峰值的承载能力，输出针对性的优化调整建议，保障数据库始终处于稳定高效的运行状态。三是网络架构合规性评估。对现有数据中心网络架构、物理架构、虚拟化架构进行全面分析、拓扑绘制、问题诊断、合理性评估，输出优化方案与改进建议，提升架构可靠性、扩展性与运维效率。四是资源使用情况评估。按季度对服务器、存储、数据库、虚拟化、网络资源使用情况进行数据采集、趋势分析、负载评估、容量预判，为资源扩容、缩容、规划提供科学依据。五是迁移方案评估。针对系统迁移、数据迁移、设备移机、虚拟机迁移等需求开展前期调研、风险评估、方案设计、可行性论证，确保迁移安全、平稳、业务不中断。六是运行管理评估。围绕日常运维全流程开展管理合规性校验，同时配套评估运维流程的规范性、操作记录的可追溯性，梳理当前故障处置环节存在的卡点短板，优化应急响应机制，保障各类故障都能在规定时限内完成处置，降低业务中断影响。

5. 硬件设备运维清单

以上所有相关工作均针对以下相关设备进行操作，确保设备安全稳定运行。

序号	产品名称	数量	运维对象类型
1	华为核心交换机	4	网络设备
2	华为汇聚交换机	1	网络设备
3	华为接入交换机	1	网络设备
4	华为存储	4	存储设备
5	华为光交换机	1	存储设备
6	H3C 核心交换机	2	网络设备
7	H3C 汇聚交换机	2	网络设备
8	H3C 接入交换机	63	网络设备
9	H3C 路由器	5	网络设备
10	H3C 服务器	8	主机设备

11	深信服负载均衡	2	网络设备
12	神州云科负载均衡	2	网络设备
13	浪潮服务器	21	主机设备
14	浪潮存储	2	存储设备
15	浪潮光交换机	2	存储设备
16	联想服务器	3	主机设备
17	戴尔服务器	1	主机设备
18	惠普服务器	2	主机设备
19	超聚变服务器	2	主机设备
20	IBM 服务器	16	主机设备
21	数据库一体机	1	主机设备
22	中间件	35	成品软件
23	数据库	25	成品软件
24	长虹光交换机	1	存储设备
25	爱数备份一体机	1	存储设备
26	操作系统	330	成品软件

2.2 安全维护服务保障

6. 数据中心日常维护

（1）数据中心日常巡检。一是运维安全监测。对业务系统、网站页面、数据内容、运行状态开展日常安全监测，及时发现页面异常、信息泄露、配置变更等风险，保障系统与数据安全。二是 7×24 小时平台告警监控。通过安全管理平台对信息系统、网络设备、安全设备进行 7×24 小时不间断实时监控，及时发现各类安全威胁、异常行为与安全告警，完成告警分级、事件响应、跟踪处置与闭环管理，保障系统安全稳定运行。三是每日安全健康巡检。每日对信息系统开展全面安全健康检查，覆盖系统漏洞、账号口令、网络访问控制等关键安全项，排查安全隐患并登记整改，确保系统安全合规运行。四是值班值守安全监控。在夜间值守时段对机房环境、系统运行、网络访问、安全事件进行不间断监控，及时发现并处置夜间突发安全问题，保障全天候安全可控。

（2）数据中心风险预防。一是每周安全巡检.每周对信息系统、网络及安全设备、安全策略、账号权限进行全面安全检查，及时发现并整改各类安全隐患，保障系统与设备安全稳定运行。二是安全性能分析。定期对系统安全运行性能、安全风险态势、网络流量情况进行分析研判，识别潜在安全风险，提升安全防护与流量管控能力。三是季度深度安全健康检查。每季度对安全设备进行全面安全合规核查、配置复核、策略校验、权限审计、运行状态评估与隐患排查，形成完整检查记录与整改建议，确保安全合规、策略有效、权限可控、运行稳定。四是备份安全验证。定期对数据备份机制、备份文件安全性、数据加密有效性进行验证检查，确保备份可用、数据安全、恢复流程可靠。五是季度安全资产核查。每季度对安全设备、安全软件资产进行全面盘点与合规核查，确保安全资产账实相符、授权合规、配置有效、运行正常。

		（3）数据中心基础运维。一是系统安全补丁更新。按照官方安全公告与漏洞修复要求，定期对操作系统、中间件、数据库、应用系统开展补丁更新作业，及时修复系统存在的安全缺陷，提升系统整体安全防护能力。二是安全设备配置备份。对各类安全设备的配置信息、安全策略进行定期备份作业，确保配置文件完整可追溯，在设备故障或策略异常时可快速恢复。三是安全日志归档清理。按照安全合规与审计要求，对系统产生的安全日志、审计日志进行规范留存、分类归档与定期清理，保证日志可审计、可追溯、合规存储。四是机房安全维护。对数据中心机房物理安全、门禁系统、安防系统进行定期维护检查，保障机房环境安全、出入可控、监控有效，防范物理安全风险。五是安全接入检查。对各类外联专线、外部接入链路、访问权限进行安全检查，保障接入链路稳定、访问行为合规、权限最小化，防范外部接入带来的安全风险。六是运维安全文档输出。按照运维管理与安全合规要求，定期输出各类安全运维文档，实现工作可记录、可检查、可追溯、可闭环。七是渗透测试服务。对系统进行一年四次渗透测试。测试内容包含系统层安全渗透测试、WEB 中间件渗透测试以及 WEB 应用渗透测试。通过渗透测试，及时发现潜在的安全风险，并加强安全防御，提高网络和系统的安全性和可靠性，保护重要的业务信息和数据不丢失。针对渗透测试的安全风险修复后进行复测，并出相关报告。八是漏洞扫描服务。对系统进行一年四次漏洞扫描服务。漏扫前期要开展常态化的漏洞扫描和基线配置核查工作，发现运行过程中可能存在硬件、软件、协议的具体实现或系统安全策略上的缺陷，从而及时消除安全漏洞可能带来的安全风险。针对漏洞扫描的安全漏洞修复后进行复测，并出相关报告。九是系统监控服务。每日进行系统监控服务，提供系统入侵攻击检测、网页篡改检测、敏感关键字内容检测、网站实时流量监测、系统备案监测，并能够对严重安全攻击提供邮件报警功能，定期出具安全监测报告，及时发现网站故障、漏洞、攻击和异常行为，并采取及时的措施防止和解决这些问题，以确保网站的可访问性、稳定性和安全性。十是安全加固服务。对系统进行一年四次安全加固。安全加固是对应用系统、网络设备、管理制度的有效补充，四者共同配合形成有效的安全防御机制。安全加固与优化服务是根据专业安全评估结果，制定相应的系统加固方案，针对不同目标系统，通过打补丁、修改安全配置、增加安全机制等方法，合理进行安全性加强。通过使用该项服务，将信息系统的网络层、主机层和应用层等层次建立符合安全需求的安全状态，并以此作为保证信息系统安全的起点。加固过程严格按照规范执行，并出具加固服务报告。提高系统、应用、网络等安全性，减少系统遭受攻击的风险，保护机密数据的安全。十一是风险评估服务。提供两次风险评估服务，风险评估是指按固定周期，就约定的信息系统范围进行安全检查，来发现信息系统在日常运维过程中可能新增加的安全隐患，分析系统运维过程的不足，并给出相应的解决建议。十二是 SSL 证书服务。为加强对公

		共服务区各系统的安全性及高可用性，对国密安全认证加速网关的SSL证书服务进一步升级，实现RSA+SM2双SSL证书部署，为更好的提高网站身份认证、HTTP业务防劫持、数据加密等安全机制。十三是电子签章服务。适配国密算法，签发国密算法证书，开展电子签章与现有政务业务系统对接，完成证书的录入、配置与调试。 **7. 数据中心响应支持** （1）服务请求支持。一是网络安全变更。根据业务实际需求提供安全端口开通服务，严格执行端口审核与高危端口管控要求，确保端口开放合规、最小化、可管控，避免因端口开放带来安全风险。二是安全配置查询。根据运维管理、安全检查、故障排查需求，提供安全配置与策略配置查询服务，确保配置信息可查、可验、可追溯，支撑安全运维与合规检查工作。三是设备移机安全支持。在设备移机、下架、上架、搬迁过程中提供安全支撑服务，开展设备安全检查与物理安全保障，确保设备在迁移全过程不损坏、不泄密、不失控。四是日常安全工单响应。接收并处理各类日常安全类工单，按照流程及时响应、处置、反馈、闭环，确保安全问题、风险隐患、配置需求得到高效处理。五是重要时期安全保障。在重大会议、重大活动、关键业务保障时段提供专项安全保障服务，落实值守、监测、处置、汇报机制，确保保障期间安全稳定。 （2）数据中心故障处置。一是安全设备修复更换。对防火墙、入侵检测、网闸、安全管理平台等安全设备的硬件故障、运行异常、功能失效等问题进行及时维修与更换，保障安全设备正常运行、安全防护能力不中断。二是系统安全异常恢复。针对系统遭受入侵攻击、非法越权、文件篡改等安全事件进行全面处置，完成系统恢复与安全加固，确保系统恢复正常并提升抗攻击能力。三是安全性能问题排查。对因网络攻击、异常流量、恶意程序导致的系统CPU、内存、带宽等性能异常进行全面排查与处置，恢复系统正常运行性能。四是网络安全故障修复。针对网络攻击、非法接入、策略失效等网络安全问题进行阻断、处置与策略恢复，保障网络边界安全与业务稳定运行。 （3）数据中心实施变更。一是安全设备硬件上线。为新增、替换、扩容的安全设备提供上线部署服务，完成设备合规准入与安全配置部署，确保安全设备按规范接入网络并正常发挥防护作用。二是安全策略调整。根据业务变更、隐患修复、攻击防护、架构优化需求，对防火墙、网闸等安全设备的策略进行优化调整，遵循最小权限原则提升防护有效性与资源利用率。三是系统迁移安全保障。在服务器、虚拟机、数据库、应用系统迁移过程中提供全流程安全支撑，开展安全评估与数据保护，确保迁移过程不泄露、不篡改、不中断、不失控。四是虚拟化平台安全加固。对虚拟化平台开展安全加固与隔离策略调整，提升虚拟环境安全性，防止虚拟机逃逸、越权访问与资源滥用风险。 （4）数据中心应急处置。一是虚拟化平台安全加固。定期

组织开展安全应急演练活动，检验应急预案有效性、应急流程顺畅度及人员协同能力，提升面对安全突发事件的快速响应与处置水平。二是重大突发安全事件处置。针对发生的重大安全事件开展全流程应急处置工作，快速控制事态、消除威胁、降低影响，保障业务与数据安全。三是7×24小时应急响应。提供全天候不间断应急响应服务，确保各类安全事件在任何时段均可得到及时受理、快速处置与闭环跟踪。

8. 数据中心性能调优

一是网络安全架构优化。结合现有网络拓扑、业务运行需求及安全合规要求，对整体网络安全架构进行梳理、分析与优化调整，强化边界防护、访问控制与区域隔离能力，提升网络整体安全防护水平与抗风险能力。二是动态化访问范围迭代升级。优化网络出口专属边界防护设备，强化流量全链路检测拦截能力，筑牢网络边界安全屏障。三是精细化网络限制管控。完善网络配置访问管控规则，全面拦截境外陌生站点访问请求，封堵非合规外联通道，避免恶意外部站点带来的风险。

9. 数据中心运行评估

一是安全资产评估。对数据中心内所有安全相关资产、账号、权限、端口进行全面盘点、核查与梳理，形成完整台账，确保资产清晰、权限合规、端口可控，为安全运维与风险管控提供基础支撑。二是容量评估。对现有安全防护体系的防护能力与安全资源承载容量进行检查、分析与评估，识别短板与瓶颈，确保安全资源满足业务运行与防护需求。三是安全通报评估。定期向用户推送安全相关信息，及时告知系统安全态势、安全风险提示及官方安全通知，为安全运维与防护决策提供支撑。四是风险评估。围绕信息系统三级等保要求，对网络、主机、数据、应用、管理等层面开展全面综合风险分析，识别安全隐患、研判威胁影响、提出可落地安全建议，并对评估报告进行逐项解读，为安全加固与运维优化提供依据，确保系统符合安全合规与稳定运行要求。

10. 网络安全培训

围绕数据中心安全运维需求，面向运维人员与相关岗位人员每季度开展一次专业化、体系化安全知识与实操技能培训，强化网络安全防护意识、提升漏洞处置、应急响应、终端防护、数据安全管理能力，培训内容贴合人社系统实际运行环境，严格按照既定频次、时长与规范流程组织实施，确保参训人员掌握必备安全技能并能落地应用。

11. 安全设备运维清单

以上所有相关工作均针对以下相关设备进行操作，确保设备安全稳定运行。

序号	设备名称	数量	运维对象类型
1	深信服防火墙	8	安全设备
2	深信服WEB防火墙	2	安全设备
3	深信服流量监控探针	2	安全设备

4	深信服日志审计	1	安全设备
5	深信服数据库审计	1	安全设备
6	深信服安全感知平台	1	安全设备
7	深信服上网行为管理	1	安全设备
8	深信服终端安全管理系统	1	安全设备
9	启明星辰 VPN 设备	4	安全设备
10	奇安信防火墙	2	安全设备
11	奇安信日志审计	1	安全设备
12	奇安信数据库审计	1	安全设备
13	天融信堡垒机	2	安全设备
14	H3C 网闸	2	安全设备
15	迪普科技防火墙	1	安全设备
16	证书签发设备	1	安全设备

2.3 其它维护服务保障

一是运维服务配套辅材供给保障.服务周期内免费提供机房运维全场景所需的各类配套辅材，包含网络运维类的六类网线、光纤跳线、水晶头、网络模块、配线架、理线器，硬件调试类的各类适配电源线、信号连接线、绝缘扎带、防静电耗材，以及日常运维所需的标签纸、清洁耗材、接口防护配件等所有低值易耗辅材。所有辅材均符合机房防火、防静电规范要求，按需随用随补，无需采购人额外承担采购成本，保障日常巡检、故障处置、设备调试等运维操作可无阻碍开展。二是故障应急备品备件支撑保障。针对机房内服务器、存储、网络、安全等核心设备，建立覆盖全品类的备品备件库，包含电源模块、硬盘、光模块等高频故障部件。所有备品备件均与在用设备同品牌、同型号、同性能等级，确保故障部件更换后可直接兼容适配。当设备硬件发生故障需离线维修时，1 小时内完成备品备件的现场替换，保障业务不中断，后续同步跟进故障部件的返厂维修流程，维修完成后及时补充备件库存，形成“故障即换、动态补库”的闭环保障机制。同时建立全量备品备件台账，详细记录备件序列号、出入库时间、更换使用记录，确保资产信息可追溯、可核对。三是数据备份移动存储介质保障。按需提供符合人社数据安全等级要求的移动存储介质，介质容量覆盖不同等级的备份场景，定期配合完成全量业务数据的离线冷备份存储，同时建立介质全生命周期管理机制，记录介质编号、存储数据内容、备份时间、存放位置，严格执行涉密数据介质的使用、归还、销毁流程，完全符合人社行业数据备份合规要求。四是安全管理正版资源与移动设备保障。提供机房重要网络节点的安全设备、业务防护组件的正版授权升级包，包含防火墙、终端安全管理软件的规则库、病毒库、特征库的实时在线升级服务，确保所有安全组件始终保持最新防护能力，漏洞补丁升级均从官方正版渠道获取。同时配套提供运维专用安全移动设备，如安全加固的运维笔记本、加密运维移动硬盘、专用移动调试终端等设备，所有移动设备仅可在人社业务专网内

使用，避免运维过程中引入外部病毒、恶意程序，保障机房网络边界安全。

三、技术要求

1.运维管理要求

本项目运维服务整体遵循 ITSS 信息技术服务标准，结合西安市人社局数据中心软硬件资产、人社业务系统搭建一体化运维管理体系，全程采用 PDCA“计划、实施、检查、改进” 闭环管控模式，持续优化服务流程，保障运维体系适配业务长期发展，稳步提升整体 IT 服务质量。项目建立响应式故障处置、主动式预防性巡检、价值式架构优化三位一体运维模式，每季度全面梳理事件、问题、变更、配置、发布、服务级别、服务报告七大核心流程，规范操作标准，实现运维全流程可追溯、可审计。

项目实行 7×24 小时全天候运维监控，区分工作日在岗与夜间驻场值守机制，非工作时段专人在岗监测机房环境、软硬件运行状态，严格落实交接班制度。系统搭建分级告警处置与标准化工单管理体系，硬件、网络、安全各类故障、业务需求统一走工单流转，做到及时受理、限时处置、按期闭环。运维方需按日、周、月、季度输出完整巡检、性能分析、资产盘点、备份验证、应急演练等报告；每季度完成全部 IT 软硬件资产盘点核对，更新设备台账，确保账实相符。定期备份网络、服务器、安全设备核心配置，系统日志、安全审计日志按规范归档留存、定期清理，满足等保审计存储要求。所有设备上线、网络策略调整、系统迁移、虚拟化资源变更、安全策略修改均执行风险评估、测试验证、上线复核全流程管控；全年组织 4 次系统宕机、网络中断、数据恢复类应急演练，出现重大突发事件提供 7×24 小时极速应急处置，最大限度降低业务中断影响。

2.硬件运维技术要求

硬件运维覆盖机房交换机、路由器、负载均衡、存储阵列、光交换机、物理服务器、虚拟化主机、灾备服务器、备份一体机及配套操作系统、中间件、数据库全品类设备，核心设备由专业认证工程师提供专属维保。

运维实行分层级常态化巡检监控：7×24 小时实时监控硬件、系统、数据库、动环平台，自动捕捉硬件故障、链路中断、资源过载、电力异常等告警并闭环处置；每日开展机房环境、软硬件全维度健康巡检；每周排查链路稳定性、硬件隐患与性能瓶颈；每月开展负载趋势分析、本地及异地备份完整性验证、区县及银行等外联专线链路检测；每季度实施硬件深度体检、全资产盘点、机房线缆规整、设备除尘标识更新。

常规运维作业包含系统漏洞补丁升级、设备配置定期备份、日志归档清理、新设备上架调试、旧设备移机防护、虚拟机资源动态扩容缩容、闲置资源回收等。故障处置可快速完成硬件部件检修更换、系统宕机与业务异常恢复、性能瓶颈定位优化；同时提供多维度性能调优，涵盖服务器参数优化、数据库索引与存储优化、虚拟化资源均衡、网络链路架构梳理、机房物理布局优化、

备份策略迭代升级。每季度开展 IT 架构梳理、资源容量评估，针对服务器、存储、数据迁移需求出具风险评估与落地实施方案，保障迁移过程业务连续、数据完整。

3. 安全运维技术要求

安全运维覆盖 VPN、防火墙、WAF、网闸、堡垒机、日志审计、数据库审计、态势感知、EDR、CA 证书等全部安全设备，构建全时段、全维度安全防护体系。实行 7×24 小时安全平台实时监测，识别入侵攻击、网页篡改、越权访问、恶意流量等风险，每日开展安全专项巡检，夜间叠加安全事件值守，常态化监测网站运行、敏感内容、访问流量，高危攻击自动邮件告警并定期输出安全监测报告。

项目配套标准化周期性安全服务：每周核查安全策略、账号权限、外联接入风险；每季度开展安全设备深度合规核查、安全资产盘点，并组织 1 次面向内部人员的网络安全实操培训。全年固定开展 4 次渗透测试、4 次漏洞扫描、4 次系统分层安全加固、 2 次等保合规风险评估，所有漏洞整改后完成复测并出具专项报告。日常开展安全补丁更新、安全设备策略备份、安全审计日志归档、机房物理安防巡检、外联接入权限管控；提供 RSA+SM2 国密双 SSL 证书部署服务，配套电子签章全生命周期管理接口，可对接业务系统。

建立安全工单响应机制，专项保障重大会议、重点业务时段网络安全；快速处置防火墙、审计设备硬件故障，针对网页篡改、网络攻击、非法接入等安全事件及时阻断、溯源、加固。所有安全设备上线、策略调整、系统迁移、虚拟化平台改造均落实安全管控，定期开展网络攻击、数据泄露类应急演练，发生重大安全事件 7×24 小时紧急处置。定期梳理安全资产、账号权限与开放端口，开展安全防护容量评估，常态化推送官方安全预警与风险通报，持续优化网络安全架构，强化区域隔离、边界防护能力，满足三级等保合规运行要求。

四、质量、安全及管理要求

1. 质量、安全要求

运维服务期内，供应商须提供 7×24 小时不间断的故障响应与技术支持服务。确保系统运行稳定、业务影响最小化，并按照《西安市人力资源和社会保障局信息中心网络与信息安全突发事件应急处置预案》要求，特制定以下故障分类标准及恢复时限要求。

1.1 故障分类与恢复时限

故障分类	故障定义	恢复时限
一级故	系统关键数据的保密性、完整性、可用性遭到严重破坏，业务中断 8 小时以上；	须在 8 小时内完成故障排查和进行临时处置，24 小时内完成故障修

障		复。
二级故障	系统关键数据的保密性、完整性、可用性遭到破坏，业务中断2～8小时；	须在4小时内完成故障排查和进行临时处置，8小时内完成故障修复。
三级故障	系统关键数据的保密性、完整性、可用性遭到轻微破坏，业务中断1～2小时，业务核心功能无法使用；	须在1小时内完成故障排查和进行临时处置，2小时内完成故障修复。
四级故障	系统关键数据的保密性、完整性、可用性未遭破坏，业务核心功能中断1小时以下，业务核心功能受影响；	须在0.5小时内完成故障排查和进行临时处置，1小时内完成故障修复。
五级故障	系统关键数据的保密性、完整性、可用性未遭破坏，业务次要功能受影响1小时以下，业务次要功能受影响。	须在0.5小时内完成故障排查和进行临时处置，1小时内完成故障修复。

1.2 处理要求

（1）即时响应：所有故障须在30分钟内完成首次响应，并启动处理流程。

（2）快速处置与技术支撑：在最快时间内定位并处理故障，积极联系资源支持或专家介入。

（3）业务优先原则：以“优先恢复业务”为首要目标，在恢复业务的前提下再进行彻底故障修复。若无法在时限内修复，须提供临时替代方案。

（4）善后整改与报告：故障解决后，须编制《故障处理报告》，分析故障原因，明确整改善后措施，并按要求提交。

2. 保密要求

服务商须签订保密协议，严格恪守保密纪律。对工作中接触的党政机关信息、业务数据、工作资料、内部文件、会议内容、技术资料等涉密信息，严禁私自记录、复制、拍摄、留存、泄露及违规使用。不得以私利、竞争、第三方牟利为目的向无关人员泄露采购人的商业秘密和党政机关保密信息，全程保障采购人数据安全、工作秘密和商业秘密不外泄、不滥用。

3. 人员配置要求

乙方应派驻10名具有本项目相关专业中级及以上专业技术水平人员提供驻场服务。

4. 设施设备配置要求

满足本项目需求

附件 2：合同费用清单

合同费用清单

序号	名称	单位	数量	单价（元）	税率	总价（元）
1	设备维护服务保障	项	1	1863000.00	6%	1863000.00
2	安全维护服务保障	项	1	1008500.00	6%	1008500.00
	合计：贰佰捌拾柒万壹仟伍佰元整（2871500.00 元）					

附件 3：保密协议书

保密协议书

甲方：西安市人力资源和社会保障局信息中心

乙方：中移系统集成有限公司

乙方因在甲方单位履行职务，已经（或将要）知悉甲方的秘密信息及数据。为明确乙方的保密及数据保护义务，根据《中华人民共和国民法典》、《中华人民共和国数据安全法》、《中华人民共和国网络安全法》等相关法律法规，遵循平等自愿、协商一致原则，自愿签订本协议，以期共同遵守。

一、定义

1.本协议所称的保密信息包括但不限于：

（1）甲方的战略规划、经营方针、投资计划、业务拓展和营销方案、经营管理方案、培训内容、制式文本等。

（2）甲方的财务预算方案、决算方案、利润分配方案、资金及融资状况、债务和担保情况、以及订立的重大合同等可能对甲方产生重大影响的事项。

（3）甲方的经营管理报告、各项规章制度、业务流程和标有密级的文件。

（4）甲方系统中用户的数据，包括但不限于用户清单、用户资料及个人信息、合作方式、定价政策、交易价格、合作协议等。

（5）甲方的招标和投标的标底、标书内容等。

（6）信息系统软硬件配置等资料信息。

（7）根据《保守国家秘密法》和有关法律法规应当予以保密的资料信息。

（8）甲方的内部规章制度规定不得泄露的资料信息。

（9）泄露后可能导致甲方利益受损的其他资料信息。

（10）甲方知道或应该合理地知道是“机密的”或“专有的”资料信息。

（11）甲方的应用技术资料、数据、软件、用户名、密码、系统结构、网络配置、源程序及主合同内容。

2.上述所指的“秘密信息”的资料形式，包括但不限于：书面文字资料、图片资料、视听资料、电子文档资料以及其他信息载体或秘密资料存在的任何形式。

3.本协议所称数据，是指任何以电子或者其他方式对信息的记录，包括甲方数据及甲方用户数据。

4.数据处理，包括数据的收集、存储、使用、加工、传输、提供、公开等。

5.数据安全，是指通过采取必要措施，确保数据处于有效保护和合法利用的状态，以及具备保障持续安全状态的能力。

6.用户数据，是指有关已辨别的或可识别自然人的任何数字的、字母的、图形的、摄影的、声学的或其它种类的信息。

二、双方权利义务

（一）甲方的权利义务

1.甲方拥有对所有数据及其衍生物的所有权利和权益。

2.甲方有权对乙方的数据安全保密行为进行监督。如果乙方违反保密信息保护义务，披露、使用甲方的机密信息及甲方数据的，甲方有权终止与乙方的合作。

3.甲方有权要求乙方采取合理步骤协助甲方遵守相关数据保护法律和其他隐私声明或政策下规定的义务。

4.甲方有权定期对驻场运维人员开展背景审查，乙方需无条件配合。

（二）乙方的权利义务

1.乙方保证其在处理甲方及甲方用户数据时，仅以履行协议的目的以及用户同意的目的及范围为限，按照相关数据保护法律的规定和用户授权同意范围处理。

2.乙方为甲方提供维保技术服务期间，应当保证甲方设备、网络、应用系统及数据的安全，并保证应用适配甲方的实际应用环境，除经甲方事前书面同意外，乙方不得以任何其它目的或用途为由，直接或间接对甲方数据进行披露、修改、加工、商业性开发利用系统限制等活动，否则视乙方违约，甲方有权追究乙方相应法律责任。

3.乙方了解并承认，甲方会将有具有商业价值的保密信息保存在由乙方维护的服务器上或终端计算机上，并且由于系统维护服务、数据备份服务等原因，乙方应保证维护的服务器、终端计算机应用有效安全。乙方应妥善保管相关设备及服务器的口令及账户信息，如果这些设备口令、帐户信息、数据等未经甲方事先书面许可披露给他人，造成甲方损失的，甲方将依法依规追究乙方责任。

4.乙方同意并承诺开展数据处理活动，应当遵守法律、法规，尊重社会公德和伦理，遵守商业道德和职业道德，诚实守信，履行数据安全保护义务，承担社会责任，不得危害国家安全、公共利益，不得损害甲方的合法权益。

5.乙方应建立健全全流程数据安全管理制度，组织开展数据安全教育培训，采取合理、足够的技术性和组织性措施保障甲方数据安全。利用互联网等信息网络开展数据处理活动，应当在网络安全等级保护制度的基础上，履行上述数据安全保护义务。所需费用全部由乙方承担。

6.乙方承诺重要数据的处理者应当明确数据安全负责人和管理机构，落实数据安全保护责任。乙方承担网络和数据安全责任、保密责任和对人员管理的主体责任，应对项目参与人员进行背景审查，应与所有合作单位及时签订安全保密协议，与所有运维人员及时签订安全保密承诺书，并定期对驻场运维人员开展背景审查。

乙方应明确网络和数据安全义务，乙方应指定一名高管作为网络和数据安全负责人。网络和数据安全负责人：易琼塔 。

7.乙方应合理限制乙方员工访问数据的权限，并保证完成以下事项：

（1）采取所有合理的步骤，为促进履行协议下义务而有需要访问甲方及用户数据时，以确保仅乙方的被授权员工有权在此限度内访问前述数据；

（2）确保乙方可访问前述数据的员工知晓、理解本协议及信息保护法律下的义务；

（3）确保乙方可访问前述数据的员工知晓甲方数据的保密性质，并采用适用于访问或处理前述数据的安保程序。

8.开展数据处理活动时，乙方应当加强风险监测，发现或得知系统（设备）存在网络和数据安全漏洞、缺陷或重大风险隐患的，可能致使甲方的数据有泄露

风险时，应当立即采取补救措施，且不得自行对外进行公布并尽快向甲方及有关主管部门报告相关泄露情况，最晚不应超过泄露事件发生后的 12 小时。

9.如有数据泄露风险产生，乙方的书面通知应包含以下事项：

（1）被泄露的数据主体的身份信息；

（2）对于所发生事件的描述，包括：泄露时间和被发现泄露的时间；

（3）泄露的范围，包括:所涉及数据的类型；

（4）乙方对泄露反馈的描述，包括：其采取的减轻损害的步骤；

（5）甲方可能合理要求的其它信息。

10.乙方对甲方重要数据处理时，应当按照规定对其数据处理活动定期开展风险评估，并向甲方报送风险评估报告。风险评估报告应当包括处理的重要数据的种类、数量，开展数据处理活动的情况，面临的数据安全风险及其应对措施等。

11.乙方应当按照《信息系统安全等级保护实施指南》对甲方的信息系统运营具体实施等级保护工作。

12.甲方信息系统的安全保护等级确定后，乙方应当按照国家信息安全等级保护管理规范和技术标准，开展信息系统安全建设或者改建工作，所需费用由乙方承担。

13.乙方应当定期对信息系统安全状况、安全保护制度及措施的落实情况进行自查。第三级信息系统应当每年至少进行一次自查，第四级信息系统应当每半年至少进行一次自查，第五级信息系统应当依据特殊安全需求进行自查。

经测评或者自查，信息系统安全状况未达到安全保护等级要求或实际应用需求未达到甲方需要的，乙方应当制定方案进行整改。

14.乙方应进行系统安全测评和网络安全加固，如该系统因遭遇网络入侵、非法使用等原因造成甲方数据泄露，乙方需承担违约责任，并且承担因此产生的全部法律后果。

15.甲方向乙方提供的数据在传输过程中，对数据产生的任何数据副本，残留数据，乙方必须在数据传输完成后及时进行清理销毁，否则一旦因为在数据传输过程中由于乙方未能及时妥善清理残留数据或者数据副本而造成关键数据泄露，引发的数据安全事故，乙方需承担因此产生的全部法律后果。

16.乙方同意并承诺，应对所有保密信息予以严格保密，履行个人信息和数据安全的各项法律法规和制度要求，数据所有权归甲方所有，未经甲方事先书面同意，乙方不能将所持有的与本协议有关的个人数据及保密信息向境内外转移或允许其他第三方机构或个人访问，不得存储、访问、修改、披露、利用、转让、向第三方提供、销毁人社数据。

17.乙方应建立并完善内部保密制度，与了解知悉本协议保密内容的人员签订保密协议；乙方应当告知并以适当方式要求其参与本项工作之雇员遵守本协议规定。

18.乙方只限于将上述数据提供给为履行本协议约定义务的乙方实施或者运维工程师等数据操作与管理人员，不得将关键数据向任何与实现数据集成对接无关的任何其他人员；乙方应确保参与数据操作和管理的乙方人员严格遵守本协议所规定之保密义务，如果数据操作人员有违反本协议规定的情况，即视为乙方之违约行为，甲方有权追究乙方相应法律责任。

19.乙方出于履行本协议的目的，可向其雇员披露前述保密信息，但接受这类保密信息之前乙方必须保证其雇员遵守本协议约定的保密义务。本保密义务不适用于法定披露义务。但法定披露义务也仅限于为满足相关法律要求所必须披露的最低程度，且乙方应在披露前将该情况通知甲方，以便甲方可以及时采取保护措施。

20.如果乙方通过书面意见证明：乙方对保密信息的透露是由于法律、法规、判决、裁定（包括按照传票、法院或政府处理程序）的要求而发生的，乙方应当事先尽快通知甲方，同时，乙方应当尽最大的努力帮助甲方有效地防止或限制该保密信息的透露。

21.当甲方以书面形式要求乙方交回保密信息时，乙方应当立即交回所有书面的或其他有形的保密信息以及所有描述和概括该保密信息的文件。

22.乙方应当按照甲方的要求采取有效的方法对保密信息进行保密，所需费用由乙方承担。

23.乙方对甲方的数据、软件、用户名、密码、系统结构、网络配置等不得泄露给任何第三方，如有违反，应当向甲方承担违约责任。

24.乙方雇员离职后，对在甲方任职期间接触、知悉的属于甲方保密信息及数据的内容，继续承担保密义务。如有违反，乙方应当向甲方承担违约责任。

25.乙方应在甲方的要求下，或在协议终止、到期后或者用户同意的目的完成后（以先到达的时间为准）立即保证其自身从事以下行为：

（1）以甲方同意的方式，销毁所有甲方及用户数据实现不能复原；

（2）以甲方同意的方式，对所有甲方及用户数据进行去识别化。

26.未经甲方事先书面同意，乙方不得以任何方式向任何其他组织或个人泄露、转让、许可使用、交换、赠与或与任何其他组织或个人共同使用或不正当使用从甲方获知的技术和保密信息。

27.乙方同意对甲方的保密信息予以与其自身类似信息同等保密的方式予以保护。

28.以下信息不应作为保密信息：

（1）在无违反义务的情况下，已被公众所知；

（2）在无违反义务的情况下，在披露前已被他方所知；

（3）在无违反义务的情况下，被一方独立的开发的信息；

（4）在无违反义务的情况下，从第三方处获得的信息。

三、保密期限

本协议所述秘密的保密期限不受主合同存续期间的限制；协议解除/终止后，乙方仍继续保守上述秘密信息，直到其成为公知信息。

四、违约责任

1.若乙方未履行本协议约定的义务，应当按甲方评估后的经济损失支付违约金。

2.如乙方因前款违约行为支付的违约金不足以弥补甲方损失的，应当承担损失赔偿责任。

3.前款所述损失赔偿按照如下方式计算：

（1）损失赔偿额为甲方因乙方的违约行为所受到的实际经济损失以及可举证之期待利益损失。

（2）如果甲方的损失依照本款第（1）项所述的计算方法难以计算的，损失赔偿额为不低于乙方因违约行为所获得的全部利润的合理数额。

（3）甲方因调查和追究乙方的违约行为而支付的合理费用（包括但不限于律师费、公证费用、合理调查费用等），应当包含在损失赔偿额之内。

4.因乙方的违约行为同时侵犯了甲方的商业秘密权利的，甲方可以选择根据本协议要求乙方承担违约责任，或者根据国家有关法律、法规要求乙方承担侵权责任。

五、不可抗力

（一）不可抗力是指协议订立时不能预见、不能避免并不能克服的客观情况，包括自然灾害，如台风、地震、洪水、冰雹；政府行为，如征收、征用；社会异常事件，如罢工、骚乱等。

（二）一方因不可抗力不能履行协议的，根据不可抗力的影响，部分或者全部免除责任，但是法律另有规定的除外。因不可抗力不能履行协议的，应当在五日内通知对方，同时在十日内提供不能履行协议的已经发生不可抗力的证明，以减轻可能给对方造成的损失。

六、情势变更

协议成立后，该协议的基础条件发生了双方在订立协议时无法预见的、不属于商业风险的重大变化，继续履行协议对于一方明显不公平的，受不利影响的双方可以与对方重新协商；在合理期限内协商不成的，一方可以请求人民法院或者仲裁机构变更或者解除协议。

七、数据权利

1.乙方承认甲方提供的上述数据始终为甲方的资产，数据的权威和所有权为甲方所有，乙方任何涉及数据侵权的行为视为违约，甲方有权追究乙方相关法律责任。

2.乙方如发生违反本协议的规定内容的行为，甲方可于任何时间终止本协议且不再向乙方提供任何数据，并要求乙方清除已经提供给乙方的所有关键数据及副本，乙方需以书面形式保证，数据清除过程没有以直接或间接等任何形式保留关键数据或数据副本。

八、送达

本协议首部当事人联系方式和联系信息适用于双方往来联系、书面文件送达及争议解决时法律文书送达。一方变更地址，应当及时书面通知对方，否则以原地址为准。

九、争议解决

（1）因履行本协议过程中发生争议，应通过协商解决；协商解决不成或无法协商解决的，向甲方所在地有管辖权的人民法院诉讼解决。

（2）协议不生效、无效、被撤销或终止的，不影响本协议中有关争议解决方法的条款的效力。

十、协议生效与变更

（1）本协议生效后，甲乙双方不得因姓名、名称的变更或者法定代表人、负责人、承办人的变动而不履行本协议义务。

（2）本协议自甲乙双方签字盖章后生效。本协议一式肆份，甲乙双方各持两份，均具有同等效力。

（3）本协议未尽事宜或对本协议的任何变更、补充及增加经协议方协商一致，可订立补充协议。补充协议、附件均为本协议不可分割的部分，与本协议具有同等效力。

（4）本协议及其附件构成各方之间关于该等合意事项全部内容，并已取代之前各方关于此合作事宜的任何口头或书面的谅解、承诺、报价或协议。

（以下无正文）

附件 4：考核标准

考核标准

服务绩效考核按照考核标准对供应商的服务进行考核，服务考核时间为服务期截止前一个月内。

服务质量考评结果：

优秀：考评得分大于等于 90 分。

一般：考评得分大于等于 60 分而小于 90 分。

较差：考评得分小于 60 分。

考核规范：

1）根据考核标准对服务质量进行考核。

2）服务质量结果评价：

当服务质量考评结果为优秀时，表示在服务期间内未发生仍何重大事件，服务质量符合要求，服务考核得分为 100 分。

当服务质量考评结果为一般时，表示在服务期间内发生 1-2 次重大事件或有多次未按规定提供一般服务，服务质量基本满足要求，服务考核得分为实际得分。

当服务质量考评结果为差时，表示在服务期间内发生多次重大事件或有多次未按规定提供重要服务，服务缺失，难以继续胜任服务工作，服务考核得分为 0 分。甲方有权单方面终止服务。

考核采取扣分制，扣分至满 100 分止。绩效考核系数计算方法：

绩效考核得分	绩效考核系数
100～90	1.00
89～80	0.90～0.80
79～70	0.79～0.70
69～60	0.69～0.60
60 分以下	0

西安市人力资源和社会保障局信息中心
2026 年度数据中心专业维保服务项目
供应商评价表

类别	服务内容	评估标准（注：扣分至满 100 分止）	扣分标准	扣分情况	备注
人员服务	人员驻场	驻场人员资质不符合招投标文件及合同要求，未按规定派驻符合要求的驻场人员提供服务	-5		
		驻场人员人数不符合招投标文件及合同要求，未按规定派驻符合要求的驻场人员数量	-5		
		驻场人员未按照甲方规定进行考勤	-1		
		驻场人员无故离开值班岗超过 1 小时,小于 1.5 小时	-1		
		驻场人员无故离开值班岗超过 1.5 小时，小于 2 小时	-2		
		驻场人员无故离开值班岗超过 2 小时	-3		
		驻场服务人员更换次数小于 2 次	-1		
		驻场服务人员更换次数大于等于 2 次	-3		
		驻场人员不服从甲方管理，违法甲方日常办公、机房管理等制度	-10		
		发生偷盗、失窃等安全事故	-20		
		收到书面投诉	-10		
	特殊时段保障	节假日：未按甲方要求提供相应服务	-2		
		临时突发时间：未及时处理解决	-5		
	远程人员	后端团队人数不满足要求，导致项目延期。	-10		
	服务态度	服务人员服务态度恶劣	-10		
		服务人员不具备责任心，响应速度差	-10		
技术服务	项目建设	建设内容不符合项目合同及招投标文件	-2		
		需求调研不详细	-2		
		设计功能不能满足用户需要	-2		
		项目验收不能一次通过	-10		
		因乙方自身原因导致项目延期	-5		
		项目变更不符合标准手续	-5		

		未按时组织项目例会	-1		
		出现数据安全保密问题	-5		
	项目文档	未按时间要求提交项目过程文档	-2		
		所写文档与实际建设内容不符	-2		
		项目月报周报未按时提交	-1		
		文件签批不符合规范	-1		
	试运行	试运行期间出现重大事故	-10		
		未按时提交试运行记录	-1		
		试运行未达到预期效果	-5		
		试运行期间未及时进行功能优化	-2		
	技术培训	未按时提供现场培训服务	-2		
		培训内容与要求不符或未到达要求	-3		
注：以上考核内容若项目不涉及则不扣分					
考核期测评总分					
建设单位项目负责人签字： 日期：		承建单位项目负责人签字： 日期：			