合同编号：UEJCA2602913EGN00

合同编号：

数字工信（一期）和陕西工业经济综合信息平台运维服务项目软件运维服务技术服务合同

甲　方：陕西省工业和信息化厅信息中心

乙　方：中电信数智科技有限公司

UEJCA2602913EGN00

合同编号：UEJCA2602913EGN00

UEJCA2602913EGN00

合同编号：UEJCA2602913EGN00

甲方：陕西省工业和信息化厅信息中心
统一社会信用代码：12610000435200204L
法定代表人/负责人：
联系地址：西安市新城区新城大院前大楼 7-021
项目联系人：廖怡
电　　话：029-63917218

乙方：中电信数智科技有限公司
统一社会信用代码：91110000710928807K
法定代表人/负责人：陆良军
联系地址：北京市海淀区复兴路 33 号 13 层东塔 13 层
项目联系人：张鹏
电　　话：010-58552665

本合同甲方委托乙方就[数字工信（一期）和陕西工业经济综合信息平台运维服务项目软件运维服务]项目（简称“项目”）进行专项技术服务，并支付相应的技术服务报酬。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》以及相关法律法规，达成如下合同，并由双方共同恪守。

第一条技术服务内容

1.1 技术服务的目标：对数字工信（一期）和陕西工业经济综合信息平台相关应用系统的运行提供持续、稳定、安全的运行保证和服务支撑，确保应用系统各项功能正常发挥，提升系统运行效率和用户使用体验，切实满足省、市、县三级工信管理部门及相关工业企业的业务需求。

1.2 技术服务的内容：对数字工信（一期）和陕西工业经济综合信息平台开展软件运行维护，保障其安全稳定运行。（详见附件一：运行维护服务内容）。

1.3 技术服务的方式：现场及远程服务。

第二条技术服务时间和地点

2.1 技术服务地点：西安。

2.2 技术服务期限：服务期 1 年，自合同签订之日起。

第三条甲方的权利和义务

3.1 甲方有权对合同规定范围内乙方的服务行为进行监督和检查，乙方运维服务部分或者全部不符合合同约定条件的，甲方有权指正，并要求乙方限期整改。

3.2 甲方应提供本项目实施需要具备的服务环境和工作条件。

3.3 根据本合同规定，按时向乙方支付费用。

第四条乙方的权利和义务

4.1 按照本合同约定履行服务内容，接受甲方监督、项目行业管理部门及政府有关部门的指导。

4.2 及时向甲方通告本项目服务范围内有关服务的重大事项。

第五条合同费用

5.1 本合同费用总额（含税价）：大写人民币[柒拾捌万捌仟元整]，¥[788000.00]；其中价款为大写人民币[柒拾肆万叁仟叁佰玖拾陆元贰角叁分]，¥[743,396.23]，增值税款为大写人民币[肆万肆仟陆佰零叁元柒角柒分]，¥[44,603.77]。

5.2 合同总费用由甲方按照以下第（2）方式向乙方支付：

（1）一次性支付

验收合格后[/]个工作日内，甲方向乙方支付本合同费用。

（2）分期支付

甲方分期向乙方支付本合同费用：

1、自本合同双方签字盖章生效之日起 30 日内，支付合同总金额的 40.00%。即大写人民币[叁拾壹万伍仟贰佰元整]，¥[315200.00]；

2、自乙方开始提供服务满 6 个月之日起的 30 日内，支付合同总金额的 50.00%。即大写人民币[叁拾玖万肆仟元整]，¥[394000.00]；

3、自本合同约定的服务期限届满，且经甲方最终验收合格之日起 30 日内，支付合同总金额的 10.00%。即大写人民币[柒万捌仟捌佰元整]，¥[78800.00]；

5.3 甲乙双方银行账户信息和纳税人信息

甲方信息如下：

开户行：[中国工商银行股份有限公司西安新城支行]

银行地址：[西安市新城区省政府院内]

户名：[陕西省工业和信息化厅信息中心]

账号：[3700021309088211197]

统一社会信用代码：[12610000435200204L]

地址：[新城省政府前大楼 7-19 号]

电话：[63917216]

乙方信息如下：

开户行：[广发银行股份有限公司北京太阳宫支行]

银行地址：[北京市朝阳区夏家园 11 号楼 1 层 4 号]

户名：[中电信数智科技有限公司]

账号：[9550880244109000130]

统一社会信用代码：[91110000710928807K]

地址：[北京市海淀区复兴路 33 号 13 层东塔 13 层 1308 室]

电话：[010-58552665]

第六条保密

6.1 为履行本合同，甲方委托乙方处理相关数据和个人信息的，双方均应当严格按照相关法律法规规定，采取措施确保个人信息处理活动符合法律、行政法规的规定，任何一方不得向第三方提供或者披露因本合同的签订和履行的有关数据和信息，法律、法规、规章或监管要求另有规定或本合同另有约定的除外。

6.2 本保密条款在服务期限内及服务终止后两年之内持续有效。

第七条合同变更

合同一经签订，不得擅自变更。如确需变更，应当由双方协商一致，并以书面形式确定。一方可以向另一方提出变更合同权利与义务的书面请求，另一方应当在收到书面请求后5个工作日内予以答复；逾期未予答复的，视为同意。

第八条验收

8.1 验收的时间和地点：服务期结束后30日内，甲乙双方组织验收。

8.2 验收依据：国家相关标准规范、合同、双方认可的其他书面约定 。

8.3 技术服务工作成果的验收标准：合同约定的业务、验收数据达到或超过本项目技术规范要求，验收方为通过。验收小组应出具《验收意见》或《验收报告》。

第九条违约责任

9.1 甲乙双方必须遵守本合同并执行合同中的各项规定，任何一方未履行或未完全履行本合同约定，均构成违约。

9.2 因乙方工作人员在履行职务过程中的疏忽、失职、过错等故意或过失原因给甲方造成损失或侵害，包括但不限于甲方本身的财产损失、由此而导致的甲方对任何第三方的法律责任等，乙方对此均应承担全部的赔偿责任。

第十条法律适用和争议解决

10.1 本合同适用中华人民共和国法律。

10.2 所有因本合同引起的或与本合同有关的任何争议通过双方友好协商解决。如果双方不能通过友好协商解决争议，则任何一方均可向[甲方住所地]有管辖权的人民法院起诉。

10.3 诉讼进行过程中，双方继续履行本合同未涉诉讼的其他部分。

第十一条不可抗力及免责

如由于战争、骚乱、恐怖主义、灾害、国家法律法规或规章变动、网络安全、网络无法覆盖、停电、通信线路被人为破坏、黑客攻击、计算机病毒侵入或发作、突发事件等，导致甲乙双方或一方不能履行或不能完全履行本合同项下有关义务时，受影响方不承担违约责任，但应当尽快书面通知对方。在影响消除后的合理时间内，一方或双方应当继续履行合同。如因此导致合同不能或者没有必要继续履行的，本合同可解除。

第十二条合同生效和其他

12.1 本合同纸质文本一式四份，甲乙双方各执两份，自双方签字盖章之日起生效；若使用电子印章的，自双方盖章之日起生效。

12.2 附件为本合同不可分割的部分，与合同正文具有同等法律效力。

附件：1.运行维护服务内容

2.安全承诺书

（以下无正文）

合同编号：UEJCA2602913EGN00

甲方：

法定代表人/负责人：

或授权代表：

签署日期：2026]年[8]月[20]日

乙方：中电信数智科技有限公司

法定代表人/负责人：

或授权代表：

签署日期：2026年[8]月[20]日

UEJCA2602913EGN00

附件 1

运行维护服务内容

一、运行维护总体要求

1.可用性要求

在服务周期内平台不出现系统崩溃、业务中断或数据丢失等重大事件，整体平均可用性≥99.9%。

2.安全性要求

确保数字工信（一期）和陕西工业经济综合信息平台运行稳定、可靠、安全、完整，避免设备损毁、信息泄漏或丢失等安全责任事故发生。

（1）避免发生因病毒、木马等外部因素造成业务系统大面积瘫痪（30%以上）的安全事件。

（2）避免发生信息被泄露并造成恶劣影响的事件。

（3）不发生三级以上信息安全事件，发生四级的信息安全事件每年不超过 2 起。

3.规范性要求

按照有关运维服务规范制定完备的规章制度，严格按照有关操作规程、服务规范等提供运维服务，在变更管理、安全事件处置、风险防范、应急管理等环节，做到制度完备、措施得当、执行到位。

4.及时性要求

及时响应服务工作中可能出现的各类事件，包括设备或系统故障、用户的服务请求、应急响应等，故障及时响应率 100%，故障及时解决率≥98%。

5.满意度要求

用户对运维服务不满意并提出投诉事件不超过 3 次，满意度≥98%。

二、运行维护内容及要求

提供运维驻场服务，驻场服务人数为 2 人，确保数字工信（一期）和陕西工业经济综合信息平台稳定运行，本项目主要服务内容包含但不限于：例行服务、故障处理服务、应急保障与培训服务、软件优化升级、安全加固服务等。

1 例行服务

包括日常监控、预防性检查、数据备份、短消息、响应支持等服务。

1.1 日常监控服务

提供运维监控工具对运行状态进行 7×24 小时实时监控，出现告警时及时排查处理，并定期对告警日志进行统计分析。根据实际运行情况及时优化配置参数，完善更新监控项，建立监控及巡检报告。

1.2 预防性检查服务

运维方需建立“日常巡检+定期巡检”相结合的巡检机制，覆盖平台应用系统全模块、全功能，确保及时发现并消除潜在隐患，实现巡检工作标准化、常态化。

1.2.1 日常巡检

每日巡检不少于 2 次，查看基础软件、支撑软件、应用软件的运行日志，功能模块运行是否正常，巡检发现异常问题应及时上报并分配维护人员进行处理。

1.2.2 定期巡检

每周 1 次全面巡检，每月 1 次深度巡检，所有巡检记录、报告需按规范归档，保存期限不少于 3 年，确保巡检工作可追溯，为后续运维优化提供依据。

1.3 数据备份服务

（1）数据存储系统运维：包括存储系统运行状态监控和预警、定期巡检维护、开关机、故障处理、调整优化、配置信息备份管理、技术文档管理等。存储系统的监控和巡检按照日常巡检工作执行。

（2）数据备份策略制定：制定科学的数据备份与恢复策略，包含备份内容、备份方式、备份周期、保留策略等内容，备份内容包含系统部署包文件和配置文件、数据库表结构、数据、存储过程、操作系统整机/镜像、中间件配置与证书、业务附件文件、SSL 证书授权等。

（3）数据备份执行：严格按照数据备份策略进行备份，每次备份后进行完整性校验；每月对数据备份进行 1 次可恢复性测试；定期清理过期备份，释放存储空间。

1.4 短消息服务

（1）定期进行短信发送测试，检查短信平台接口的发送功能，查看是否存在告警或错误信息，对异常信息进行排查分析，并创建事件记录。

（2）根据账号密码更新情况及时维护短信平台账号，保障短信发送畅通。

（3）查看、统计已发送的短信数量，短信计费、余额情况。

1.5 响应支持服务

通过热线、交流咨询群、邮件、主动回访等方式为用户提供咨询、投诉、故障申报、业务受理等服务，并将所有问题记录。对于用户申报的请求和故障，运维方须在 30 分钟内向用户反馈处理进度或处理结果，对于不能及时处理的事件及时向用户进行说明。

（1）热线服务：通过服务热线解决日常使用问题，提供应用建议，并将所有电话问题记录。5×8 小时服务。

（2）交流咨询群服务：运维方通过微信群、QQ 群解决用户提交的问题，并将所有问题记录。7×8 小时服务。

（3）邮件服务：运维方通过邮件解决用户提交的问题，并将所有问题记录。7×8 小时服务。

（4）主动回访服务：定期主动回访用户，了解使用中存在的问题及对产品、服务的建议。

2 故障与问题处理

2.1 故障处理服务

2.1.1 故障处理范围

故障处理范围包括但不限于以下情况：

（1）负责用户使用操作问题指导；

（2）负责由于网络环境、病毒入侵、系统资源不足引起的故障修复；

（3）负责由于平台参数设置问题引起的故障修复（如支撑软件系统等）；

（4）负责由于业务数据录入、接口配置、用户权限配置问题不正确引起的故障修复；

（5）配合平台涉及主机操作系统、数据库、中间件问题引起的故障修复；

（6）负责由于开停机操作系统崩溃引起的故障修复；

（7）负责由于平台的迁移、重新部署引起的故障修复；

（8）配合由于第三方软件或中间件版本问题引起的故障修复；

（9）负责根据业务发展需要对业务系统常规参数进行配置调整（包括集成接口的配置调整、权限的配置调整、业务参数的配置调整等）；

（10）配合平台本身以及涉及到的所有相关软件升级操作；

（11）负责编制典型故障的分析报告和处理过程文档；

（12）配合处理突发性的信息安全事件并负责编制应急处置方案等相关文档；
（13）负责定期进行故障分析，并出具分析报告及建议；
（14）负责根据实际需要更新预防性维护计划；
（15）负责根据业务系统实际需要完善数据备份机制及恢复机制；
（16）负责完善平台运维过程中资料的更新；
（17）负责完成各业务系统漏洞修复、补丁安装等；
（18）负责完成其他不可预知的问题引起的故障修复。

2.1.2 故障处理流程

（1）故障事件登记记录和上报：接收到故障事件报告或发现故障后，及时对事件进行登记记录并上报项目负责人，通知省工业和信息化厅信息中心。

（2）故障事件判断、响应与处理：项目负责人对事件进行初步判断，确定事件级别，并安排人员对事件进行响应。对于四级事件，由驻场人员响应处理；对于三级及以上事件，应根据故障类型指派对应技术工程师响应处理。

（3）故障事件升级：对于事件响应要求的时间内无法完成处理的事件，应派遣更高一级技术人员或报告更高一级管理人员给予支持。

（4）故障恢复与验证：故障处置完成后，应对系统功能、运行状态进行验证，确认故障已解决，系统恢复正常。同时通知省工业和信息化厅信息中心，由省工业和信息化厅信息中心进行确认。

（5）故障记录与复盘：故障处置完成后，详细编制故障报告，包括但不限于故障原因、处置措施、处置结果、恢复时间等信息。定期对故障进行汇总复盘，分析故障规律，提出防范措施。

2.1.3 故障处理时间要求

所有事件按重要性、严重性和紧急程度综合考虑分为四个等级，一级为最高，故障处理时间要求：

故障级别	核心判定	响应要求
一级 （特别重大故障）	系统核心功能全面中断，如工业大数据库无法正常读写、核心业务应用全面不可用，影响业务用户数量≥50%。系统关键数据的保密性、完整性、可用性遭到严重破坏，并造成恶劣影响的。	2 小时内必须恢复核心功能
二级 （重大故障）	系统部分核心功能中断或严重异常，如部分业务应用无法使用、数据采集/同步大面积失败、系统性能严重下降，响应时间超过 10 秒，错误率>50%，20%–50%用户受到影响。	4 小时内恢复
三级 （较大故障）	系统非核心功能异常，如个别页面显示异常、非核心接口调用失败，对业务开展影响较小，小范围用户受影响，可临时规避。	1 个工作日内恢复

四级 （一般故障）	系统操作体验类问题，如页面加载缓慢、个别功能操作繁琐、非核心数据显示错误，不影响业务正常开展。	3 个工作日内或 下一个版本迭代修复

2.2 变更管理服务

在运维过程中会涉及变更操作，如系统参数调整、软件版本更新、系统性能评估、系统性能优化、软件缺陷和错误修正、软件参数配置及性能优化、数据更新等纠正性、预防性、适应性维护操作，需按变更管理流程进行管理。

变更管理流程：

（1）变更申请：提出变更需求，说明变更操作、变更原因，提交省工业和信息化厅信息中心。

（2）变更评估：对变更需求进行技术评估，分析变更可能带来的风险，制定变更方案、测试方案及回退方案。

（3）变更审批：省工业和信息化厅信息中心对变更方案进行审批，审批通过后方可实施变更。

（4）变更实施：在非工作时段实施变更，严格按照变更方案执行，做好变更记录，实施过程中若出现异常，立即启动回退方案。

（5）变更验证：变更实施完成后，运维方及省工业和信息化厅信息中心对变更结果进行验证，确认变更达到预期效果，系统运行正常。

（6）变更归档：将变更申请、变更方案、测试方案、回退方案、操作记录等资料归档留存，形成完整的变更档案。

3 应急保障及培训服务

3.1 应急保障服务

（1）编制应急预案：编制可操作、有针对性的网络与信息安全应急预案，当突发安全事件时应按照应急预案处置措施尽快恢复受影响的业务系统。

（2）组织应急演练：制定演练计划和演练方案，定期进行应急演练，演练时要做好演练记录、演练评估和演练总结。

（3）安全事件处置流程：当发生安全事件时，应立即采取措施控制事态，必要时采用断网、关闭服务器等方式防止事态进一步扩大；根据应急预案立即开展工作，将事件造成的影响控制在最小范围；在应急处置工作结束后，应对本次应急事件处置工作进行回顾，形成《突发事件应急事件报告》。

3.2 培训服务

根据省工业和信息化厅需求，为用户提供答疑、演示和培训服务，帮助用户熟练掌握平台使用。每年至少为平台使用人员开展一次业务培训，培训内容涵盖平台操作、日常问题排查、安全注意事项等，培训人员覆盖省、市、县三级工信主管部门和部分企业。

4 软件升级服务

提供平台小版本迭代升级服务，包含功能优化、缺陷修复、体验提升；升级前评估兼容性、风险点，做好数据备份与环境准备；升级过程平稳实施，分步部署、测试验证；确保升级后功能正常、数据完整、业务不中断；提供升级说明文档，同步更新培训内容与操作规范。本次运维内容包含但不限于以下升级服务：

（1）工业运行报告生成

实现工业运行数据一键导入系统，基于工业运行报告标准模板，自动完成数据回填匹配，直接导出工业运行报告。

（2）智能工厂梯度培育储备库

实现制造业企业线上填报并提交摸底调查表，由区县、市两级逐级审核，先形成基础级企业推荐名单；名单汇总上报省级后，经省级复核审定，最终生成先进级企业名单。

（3）“一企一档”

平台建立一企一档，每个企业都建立一个档案，就是企业在平台所有的数据痕迹，申报的项目数据，运行数据、基础数据等一切数据，每个企业建立一个档案。

（4）项目申报系统提升

针对现有项目申报系统进行优化升级，包括：支持按行政区划、申报时间多维度对全部项目数据开展统计分析，通过图表可视化方式直观呈现各维度下扶持项目数量、补助扶持资金总额等关键指标；以制造业技术改造升级项目为例实现系统全流程线上管理。

（5）工信厅信用子系统优化

在自然人行政处罚以及法人行政处罚指标信息中增加信用中国双公示系统中新增的字段，并与信用中国实现接口互通。

（6）陕西清欠投诉线索办理系统优化

陕西清欠投诉线索办理系统中的指标需与国家清欠投诉系统的指标保持一致，导出文件时需确保全量数据完整导出；实现国家清欠投诉系统导出数据的统计汇总功能；首页增加企业可查看政策的功能；将“待初审线索平台”小程序嵌入到系统中。

（7）省级高新区数据填报系统

实现省级高新区园区每季度首月底前按期完成季度运营数据报告的在线填报提交，同时按年度节点开展全年相关评价指标数据的集中填报工作。

5 其他服务

5.1 安全加固服务

开展系统安全评估，检测漏洞、弱口令、非法访问、注入风险等安全问题；进行操作系统、数据库、中间件、应用层安全加固；配置防火墙、访问策略、权限管控、日志审计；定期更新安全策略，开展渗透测试与安全扫描；提升平台抗攻击能力，保障数据安全与业务安全。

（1）系统状态巡检;

（2）系统性能指标查看;

（3）系统的日志记录、告警检查、问题及时上报;

（4）配合用户进行等级保护测评和国密应用安全性评估及安全检查，针对系统和网络中存在的安全漏洞、配置错误、设计错误等安全问题进行安全性加固和修复。

5.2 软件性能优化服务

分析系统响应慢、并发卡顿、查询超时等性能问题；调整服务器参数、内存分配、线程设置、缓存策略；优化接口响应速度、文件传输效率、报表生成速度；进行压力测试与并发验证，提升平台承载能力与运行流畅度。

5.3 运行环境支撑运维服务

信创云管理平台及组件运行状况进行巡检，配合云平台运维人员对云平台数据库和操作系统等信创云平台进行维护，提供相应的支持与配合服务，共同解决信创云可能出现的故障。

5.4 完成甲方交办的与本项目业务系统运行、使用相关的其他工作。

6 运维文档管理

运维方应建立完善的运维文档体系，确保文档真实、完整、规范、可追溯，所有文档需分类归档，妥善保管，定期更新；同时按省工业和信息化厅信息中心要求，定期提交相关文档。

合同到期后15天内提交纸质版维保工作总结报告，封面及骑缝加盖公章，总结报告内容包括但不限于：全年维保工作概述及总结、提供相关的证明材料（软件维护记录、故障处理报告、巡检记录、软件升级、配置变更、重保期值守记录、运维周报、运维月报等）。

UEJCA2602913EGN00

附件 2

安全承诺书

陕西省工业和信息化厅信息中心：

本单位郑重承诺遵守本承诺书，如有违反本承诺书有关条款的行为，本单位承担由此带来的一切责任。

一、合规守法承诺

本单位承诺遵守《中华人民共和国网络安全法》《中华人民共和国数据安全法》《中华人民共和国个人信息保护法》《全国人民代表大会常务委员会关于加强网络信息保护的决定》《中华人民共和国计算机信息系统安全保护条例》《计算机信息网络国际联网安全保护管理办法》《互联网信息服务管理办法》《非经营性互联网信息服务备案管理办法》《移动互联网应用程序信息服务管理规定》《网络信息内容生态治理规定》《电信和互联网用户个人信息保护规定》《公共互联网网络安全突发事件应急预案》《关键信息基础设施安全保护条例》和《网络安全审查办法》及有关法律、法规、规章和政策文件规定（“相关规定”）。

二、运维权限与操作安全承诺

1. 严格遵循最小必要、授权使用原则，仅在甲方授权范围内使用系统账号、服务器权限、数据库权限、网络运维权限，绝不私自申请、破解、复制、转借、提升运维权限，绝不私自新增系统账号、后门账号。

2. 所有后台运维、代码修改、配置变更、端口调试、服务器启停、数据库操作等高危操作，必须提前向甲方报备，经甲方管理人员同意后操作，全程留存操作日志、截图记录，留存期限不少于 1 年。

3. 严禁运维人员私自外接 U 盘、移动硬盘、私人电脑、手机等外接设备接入甲方内网、业务服务器；严禁私自将甲方内网外网互通、私自修改防火墙、网关、访问白名单等网络安全配置。

4. 离岗、轮岗运维人员第一时间注销全部运维账号、收回系统权限，同步完成工作交接、安全交底，杜绝离职人员留存后台访问权限。

三、业务数据与信息保密承诺

1. 运维服务全过程接触的甲方业务数据、台账资料、用户隐私信息、财务数据、涉密文件、系统源码、架构图纸、账号密码、运营数据等全部信息，均属于甲方保密信息，我方承担永久保密义务。

2. 严禁运维人员私自下载、拷贝、截图、导出、外传、售卖、分享甲方任何业务数据、敏感信息；严禁私自复刻数据库、备份系统源码、留存甲方系统密钥、加密证书。

3. 运维所需系统备份、数据调试备份，仅限甲方指定设备存储，禁止存储至私人云端、私人设备、第三方外网服务器；运维调试完毕后，立即销毁临时调试数据。

4. 未经甲方许可，绝不向任何第三方（含我方非运维工作人员、合作单位、外部机构）披露甲方系统漏洞、网络架构、运维密码、安全防护短板等核心信息。

5. 服务期满、合同终止后，我方无条件删除全部留存甲方数据、系统资料、运维文件，不得留存任何副本，主动配合甲方完成权限回收、资料核验工作。

四、系统运维安全防护承诺

1. 常态化做好软件漏洞扫描、补丁升级、病毒查杀、防火墙运维、访问风控工作，定期排查程序 BUG、端口漏洞、权限漏洞，及时修复高危安全缺陷，防范非法入侵、越权访问。

2. 建立应急处置机制，若发现系统异常、网络攻击、数据篡改、违规登录等安全风险，第一时间阻断风险、留存日志证据，2 小时内上报甲方，配合甲方完成溯源、处置、复盘工作。

3. 规范软件迭代、版本更新、功能运维流程，所有程序修改、优化升级均经过安全检测，绝不上线带后门、带漏洞、捆绑恶意程序的程序版本，保障系统稳定、数据完整。

4. 定期配合甲方开展数据异地备份、容灾备份，保障业务数据可恢复、可溯源，避免运维操作导致数据丢失、损毁。

五、人员管理安全承诺

1. 我方对全部派驻运维人员开展背景审核、安全培训、保密教育，留存运维人员身份证、劳动合同、保密协议备案，无违法前科、网络犯罪前科人员方可入驻运维。

2. 专人专岗运维，人员变动提前 7 个工作日告知甲方，完成权限交接、安全交底，未经甲方同意不得随意更换驻场运维人员。

3. 约束运维人员履职行为，严禁利用工作便利偷窥、篡改、删除甲方业务数据，严禁干预甲方正常业务流程。

六、安全事件上报与应急承诺

1. 发生数据泄露、系统瘫痪、网络入侵、恶意篡改、病毒感染等一般安全事件，即刻止损并上报甲方；发生重大网络安全事件，第一时间固定证据，按法规要求同步上报属地网信、公安监管部门，绝不瞒报、迟报、漏报、隐匿销毁证据。

2. 全力配合甲方及监管部门开展安全事件调查、溯源、整改工作，承担运维环节对应的全部整改工作。

七、其他约定

1. 本承诺书有效期：自签署之日起，至本次运维服务终止、所有涉密信息保密义务履行完毕为止。

2. 本承诺书一式两份，甲方、承诺运维单位各执一份，签字盖章后生效，具备同等法律效力。

3. 未尽事宜，遵照国家网络信息安全法律法规及双方运维合同约定执行。

承诺单位（盖章）：

UEJCA2602913EGN00

法定代表人、负责人或授权代表（签字）：

UEJCA2602913EGN00