2025年贵州省医疗保障信息平台建设项目安全运维服务项目合同

甲　　方：　贵州省医疗保障局

乙　　方：　贵州大数据产业集团有限公司

签订时间：　2025 年　8 月　5 日

签订地点：　贵州省贵阳市

本合同由以下双方共同签署：

甲　　方：贵州省医疗保障局

法定代表人：王文忠

通信地址：贵州省贵阳市云岩区浣纱路157号

邮政编码：550001

开户名称：贵州省医疗保障局

开户银行：贵州银行贵阳浣纱路支行

账　　号：0167001800000028

纳税人识别号：/

联 系 人：李杰

联系电话：0851-85945095

传　　真：/

乙　方：贵州大数据产业集团有限公司

法定代表人：张平

通信地址：贵州省贵阳市贵阳国家高新技术产业开发区长岭街道黔灵山路357号德福中心A4栋21-23楼1-8号

邮政编码：550081

开户名称：贵州大数据产业集团有限公司

开户银行：中国银行贵安新区分行营业部

账　　号：133032073514

纳税人识别号：91520900324716 73Q

联 系 人：高圣哲

联系电话：18002075911

传　　真：/

【注：本合同双方的账户名称、开户银行、银行账号以本合同提供的为准，如有变更，变更一方应在距合同约定的相关付款期限届满二十五天前，以加盖财务专用章的书面文件通知另一方；否则视为变更无效，一切不利后果由变更方自行承担。】

甲、乙双方根据经省大数据局组织评审通过的《2025 年贵州省政务信息化运维项目实施方案（贵州省医疗保障局分册）》的标准和要求以及“2025 年贵州省医疗保障信息平台建设项目安全运维服务项目”采购文件、响应文件等采购过程中确定的有关内容，以及《中华人民共和国民法典》《中华人民共和国政府采购法》《省政府办公厅关于印发贵州省省级政务信息系统建设管理办法的通知》（黔府办函〔2023〕2 号）等有关法律、行政法规，本着诚实信用、平等双赢、长期合作、共同发展的原则，经友好协商一致，就 2025 年贵州省医疗保障信息平台建设项目安全运维服务项目签订本合同，以兹共同信守。

一、服务内容

（一）甲方委托乙方实施运维服务的项目（以下简称“项目”）概况如下：

1、项目名称：2025 年贵州省医疗保障信息平台建设项目安全运维服务项目

2、项目地点：贵州省医疗保障局指定地点

3、运维服务内容

序号	项目名称	运维内容及指标
一	贵州省医疗保障信息平台建设项目安全运维服务项目	（1）运维内容：为省医疗保障局信息平台数据中心及局大楼机 关机房提供日常安全运维、专项安全运维服务、重大活动保障、 风险评估服务、渗透测试服务、攻防演练服务、安全培训服务。 其中日常安全运维通过安全运维人员对系统平台进行的日常安 全监测与预警、安全分析与响应、安全通报与处置等运维工作，安全监测与预警包含资产发现、安全监测和安全预警，安全分 析与响应包含安全分析、取证溯源和应急响应，安全通报与处 置包含通知与通报、安全事件处理和安全加固及策略优化等。 （2）运维指标：提供 7×24 小时网络安全监测及其他相关安全 技术服务，保证维护电话通畅。对服务期间的突发安全事件、 安全产品使用优化、安全产品

		故障等问题提供良好的技术支持 和解答，并在 2 小时内予以解决、答复； 当进行初步诊断后， 依据诊断结论由技术人员通过现场+远程支持进行维护，如确需 到现场解决问题，安全运维总部保证技术人员 24 小时内到达， 并排除系统故障。
1	日常安全运维	资产发现服务： （1）服务内容：提供针对贵州省医疗保障信息平台网络侧暴露 资产的探测和全生命周期管理，对未知资产的首次发现进行脆 弱性标记的服务，资产类型包括主机、网络设备、安全设备、 数据库、中间件、应用组件等。资产发现服务主要基于网络扫 描、搜索引擎、互联网基础数据引擎等主动探测在互联网上暴 露的资产，发现未知资产，形成明确的资产清单， 同时提供网 络侧暴露资产的全生命周期管理及对未知资产的首次发现进行 脆弱性标记的服务，对每个业务梳理分析，结合业务特点对资 产重要程度、业务安全需求进行归纳，形成对互联网暴露面以 及敏感信息进行全面梳理分析，根据分析结果，定位未知安全 风险，排查风险影响范围，协助用户收敛暴露面，提高用户整体防御能力。 （2）服务目的：资产管理是网络安全领域重要的起点功能，资 产扫描也是攻击者进行攻击的第一步，对于自身资产的理解是 做好网络安全的根基；根据资产暴露情况和威胁情况梳理结果， 对由资产、敏感信息暴露在公网而产生的风险进行有效管理， 提升用户对自身资产的掌控能力；
2		安全监测服务： （1）服务内容：通过安排固定安全服务人员在运营

		中心 7×24 小时值守，负责日常安全监测，对安全监测过程中使用到的运 行工具进行维护及管理，及时对工具进行特征库更新及版本升 级，并对工具的授权等信息进行管理。 （2）服务目的：提供 7*24 小时全天候、全方位的安全监测服 务，对于异常状况及时预警，保障用户网络和系统安全
3		安全预警服务： （1）服务内容：安全预警需根据收集的风险数据提供网络安全 风险的趋势分析报表，包括漏洞的分布范围、受影响的系统情 况、可能的严重程度等内容；根据监控的安全事件提供网络中 主要的攻击对象分布、攻击类型分布等分析；能够根据预先定 义数据格式、预警信息的级别和类型等策略，自动生成预警信 息，并以预定方式通知相关人员，预警信息存档，并可提供查 询。 （2）服务目的：对于检测到的网络威胁事件，会在 30 分钟内 通过邮件、微信、电话的方式通知用户，并提供详尽的攻击信 息，协助用户改进或加固系统，防范网络攻击。
4		安全分析服务： （1）服务内容：安全分析包括安全事件分析、恶意文件分析、 脆弱性分析、全面威胁分析等内容，主要目的是对安全运营范 围内的安全信息和安全事件等进行分析，使平台管理人员更好 地了解相关信息，并及时采取相应的策略来降低安全事件带来 的安全风险。 （2）服务目的：通过安全分析服务，定期分析并筛

		选有价值安 全事件，并通知用户采取有效措施降低安全风险。
5		取证溯源服务： （1）服务内容：通过建立取证溯源机制，可以更好地理解黑客 的攻击行为和作案特征， 同时通过关联分析和可视化呈现，可 以直观的了解网络的薄弱点，从而更好地做出安全决策。通过 收集安全日志，分析网络流量等方式获取、保存和分析网络中 的安全数据，可以为取证溯源提供大量的数据，结合机器学习，从而更好地进行取证分析。 （2）服务目的：通过溯源取证，还原攻击过程，发现潜在的、 隐蔽的攻击路径，从而为后续提升安全保障提供依据。
6		应急响应服务： （1）服务内容：对各种意外事件的发生所做的准备以及在事件 发生后所采取的措施。通过建立安全事件响应机制来快速检测 安全事件、把损失和破坏降低到最低限度、弥补那些被利用的 缺陷、并恢复信息服务。 （2）服务目的：提供应急预案、进行用户网络系统安全检测和 分析，掌握系统安全状况并排除问题，进行相应的安全能力部 署和升级
7		安全事件处理服务： (1)服务内容：对发生或者发现的安全事件进行处理，对信息系 统运行时出现的各类重大安全问题、系统故障进行及时有效的 分析排除，输出相应的安全事件处理报告，降低因安全事件导 致的安全风险。 （2）服务目的：及时有效的对安全时间进行快速处置，处置方 式包括切断攻击路径，遏制攻击发展，降

		低安全事件的影响范 围。
8		安全加固和策略优化服务： （1）服务内容：通过专业的检查工具和评估方法，提供安全加 固建议并对相关系统进行加固，消除信息系统上存在的已知漏 洞，提升关键服务器、核心网络设备等重点保护对象的安全等 级。同时，根据安全运营的实际情况和特定需求，对安全运营 的监测，分析和处置等安全策略进行优化设计，使安全运营工具和服务更好地作用于安全运营工作。 （2）服务目的：提供利用 0day 和 1day 的高级威胁与定向攻击， 依托专业团队的高级分析能力，沿用安全预警工作成效，对客 户安全设备（IPS、WAF、UTM、NGFW 等）进行安全加固或配置调 整的优化服务，从而降低安全风险。
9	专项安全运维服务	业务系统安全基线： （1）服务内容：根据国内外的安全标准和最佳实践，建立基于 业务生命周期的业务系统安全基线，保障业务系统达到一定程 度的安全标准，业务系统安全基线主要包括物理安全基线、管 理安全基线、网络安全基线、主机安全基线、虚拟化安全基线、 应用安全基线和数据安全基线。根据安全核查情况，提出安全 整改建议，对基线核查内容的结果进行汇总编制《安全基线核 查报告》。每 1 年开展 2 次服务。 （2）服务目的：提供对客户主机操作系统进行全方位的基线加 固和组件升级、修补系统潜在的各种高危漏洞、解决系统中隐 藏的安全威胁的安全加固服务，从而提升安全能力。
10		安全建设管理：

		（1）服务内容：针对在信息系统进入运行阶段的管理，主要从 环境管理、资产管理、介质管理、设备管理、网络安全管理、 系统安全管理、恶意代码防范管理、密码管理、变更管理、备 份与恢复管理、安全事件管理和应急预案管理等方面入手，根 据系统平台的实际情况建立相关的安全运维管理基线。每 1 年 开展 2 次服务。 （2）服务目的：基于贵州省医疗保障信息平台的组织业务和安 全现状，根据网络安全相关标准规范、法律法规，参考国内外 网络安全管理最佳实践和理论，为用户提供全生命周期、多维 度的安全调研、分析、规划和体系建设等安全建设管理服务，帮助用户建立立体化的网络安全管理体系。
11	重大活动保障	（1）服务内容：在数博会、国庆、两会、重大国际和国内重大 活动和重要节假日等重大活动期间，加强贵州省医保局医保云 平台的驻场和二线人力保障。 1)确定重要活动保障服务目标及范围，组建重要活动保障服务 团队； 2)为开展重要活动保障，制定总体工作计划，针对在重要活动 安全保障时期提供保障前检查与整改工作，提供《安全保障方 案》； 3)针对在重要活动安全保障时期提供保障中预警与监控工作， 提供《安全保障日报》； 4)针对在重要活动安全保障时期提供保障后总结与分析工作， 提供《安全保障总结报告》。 (2)服务目的：提供重大活动期间、节假日期间的安全值班值守 保障服务，提供重大活动、节假日期间的安全保障能力，确保 业务在重大活动、节假日期间的连续、稳定和安全运行。

12		风险识别及风险矩阵： （1）服务内容：按照 GB/T 20984-2022《信息安全风险评估办 法》， 对单位的网络安全架构、信息系统所面临的威胁、存在 的弱点、造成的影响，以及三者综合作用所带来风险的可能性 的评估，形成安全风险矩阵，从而提供业务系统安全风险排查 的风险评估服务，并从技术角度分析出业务中存在的安全问题，指导客户进行加固和修复。风险识别服务可以准确了解信息系 统安全风险现状，明晰信息安全需求的同时，可以通过针对性 制定信息系统安全策略和风险解决方案，指导未来的信息安全 建设规划和投入，确保信息系统满足合规要求和业务发展安全 保障要求，为单位建立健全网络信息安全保障体系。每年开展 2 次服务。 （2）服务目的：通过对风险评估基本要素的评估，形成包括资 产、威胁、脆弱性和安全措施的风险矩阵，从而实现资产的有 针对性的保护措施。
13		代码审计服务： （1）服务内容：采用代码审计工具结合人工研判对系统源代码 进行扫描、分析和审计，寻找系统源代码中存在的薄弱环节和 业务逻辑问题、漏洞等，并提供代码加固建议和针对已加固的 问题代码进行复审（一次）。从根源先于黑客发现系统的安全 隐患，提前部署好安全防御措施，保证系统的每个环节在不同 的环境下都能经得起黑客挑战，进一步巩固用户对自身信息系 统的信赖。系统正式上线前或者系统发生需求变更并正式部署 运行之前都应当开展代码审计服务。每年开展 2 次服务。 （2）服务目的：源代码安全审计能够对整个信息系

		统的所有源 代码进行检查，从整套源代码切入最终明至某个威胁点加以验 证，以此明确整体系统中安全隐患点，协助用户开发人员提供 安全问题的解决方案，完善代码安全开发规范。
14	渗透测试专项服务	渗透测试专项服务 （1）服务内容：是为了证明网络防御按照预期计划正常运行而 提供的一种机制。主要以通过人工模拟黑客攻击的方式对指定 的远程或者本地信息系统的安全脆弱性进行检测，发现可利用 漏洞的一种安全检测行为，及时发现信息系统的漏洞和风险。 对贵州省医疗保障局的平台、系统及网络按每半年 1 次开展渗透测试服务工作，可以使得信息系统的管理人员了解入侵者可 能利用的途径，直观的了解系统真实的安全强度。能够真正未 雨绸缪，主动发现安全问题并在第一时间完成有效防护，让攻 击者无机可乘，进而避免由于网络黑客攻击造成重大损失。 1)开展信息收集工作，确认渗透测试服务业务系统及网站系统； 2)经用户授权确认渗透测试范围、时间及地点后，严格按照渗 透测试授权要求开展测试工作。 3)渗透测试过程中， 当业务系统出现可用性异常情况，应及时 暂停测试动作，排查是否因测试导致，根据业务系统实际情况 降低测试影响。 4)在进行渗透测试过程中，发现可利用漏洞后，能否对其更进 一步利用以及利用需向用户单位请示，明确此次测试的最大限 度，否则将按照点到为止原则进行漏洞探测。 5)根据渗透测试情况，对发现漏洞提出安全整改建议，按系统 分类进行整理，提供《安全渗透测试报告》；

		6)经漏洞整改后，按需开展存在漏洞部分渗透测试情况复测验证工作。 对贵州省医疗保障局的 8 个平台及 25 个子系统、2 张网络每半 年开展一次渗透测试服务，每年开展 2 次服务。 （2）服务目的：渗透测试可以模拟攻击者的攻击方式，检测网 络系统、应用程序或设备的安全漏洞和弱点，及时发现和解决 潜在的安全问题，避免因安全漏洞导致的数据泄露、信息丢失 等安全问题，以评估企业的安全防御能力，发现安全漏洞和弱 点，并提供改进建议，以加强企业的安全防御能力。
15	攻防演练 服务	由于系统本身存在脆弱性，如软件漏洞、硬件故障、人员安全 意识不足等， 同时也面临来自内部和外部的众多威胁，如内部 人员恶意破坏、外部网络黑客、病毒等恶意程序、各种自然灾 害等，面对这些风险，通过在真实环境下使用统一的攻防演练 平台开展攻击和防守，并在严格审计、全程留痕的情况下开展 攻击行为，可识别安全威胁。每年开展 2 次。
16	安全培训 服务	安全意识培训： （1）服务内容：对贵州省医疗保障局的相关业务人员进行安全 意识宣贯，为单位网络和信息安全管理的主要执行人员、系统 运维人员等提供安全相关法律法规和日常安全威胁防范措施的 培训，提升网络和安全意识，提高面临信息安全威胁严峻挑战 时的应对能力。有效提升全体人员的网络信息安全意识、保密 意识；落实网络安全法对信息安全教育培训的要求；帮助单位 的工作人员了解和掌握基本的信息安全知识，从而真正提升全 员在工作和生活中的安全意识。出具

		《安全培训计划》、《安 全培训教材》， 详细列出本次培训的课件和培训的计划，针对 性开展培训，每年开展 2 次安全技能培训。 （2）培训范围：贵州省医疗保障局管辖全省两定机构以及相关 供应链厂商。现场人数 50~100 人，远程培训（视频会议方式） 人数 500+
17	机关大楼安全运维	1. 局机关大楼互联网：定期对机关大楼互联网终端开展安全基 线核查与整改、互联网接入终端病毒库更新及漏洞扫描工作， 每季度一次。 2. 局机关大楼医保网：定期对机关大楼医保网终端开展安全基 线核查与整改、医保网接入终端开展病毒库更新、漏洞扫描工 作，每季度一次。 3. 局机关大楼政务外网：开展机关大楼政务外网安全运维工作， 包括对准入控制系统，一机两用系统，IPS 系统的日常运维；开 展日常机关大楼政务外网终端准入控制工作，依托于一机两用， IPS 系统开展日常安全监测工作。并定期对机关大楼政务外网终 端开展安全基线核查与整改以及漏洞扫描工作，每季度一次。 4.定期开展终端安全分析工作并出具分析报告，每季度一次。
18	APP 安全加固	针对 APP 隐私合规和网络数据安全提供专业可靠的安全服务， 防止应用被逆向分析、反编译、二次打包，防止嵌入各类病毒、 广告等恶意代码，保障开发者和用户的利益不受损害。

二、服务期限

服务期限：12 个月（2025 年 1 月 1 日至 2025 年 12 月 31 日）

三、服务资费标准及付款方式

（一）甲乙双方间发生的一切费用均以人民币结算支付，对应项目款项由甲方根据项目资金情况，以银行转账、电汇、银行承兑汇票等方式支付至乙方在本合同首页指定的账户，款项均为无息支付。

（二）甲方应按照本合同注明的期限、方式、币种，向乙方支付报酬。完成具体项目的实施工作后，依据具体项目的付款要求进行付款。

1、本项目服务费用含税价为：人民币￥1945700 元（大写：壹佰玖拾肆万伍仟柒佰元整)。

2、乙方在合同签订后【30】个工作日内，须向甲方以银行转账方式交纳合同金额的 10%，即人民币：￥194570 元（大写：拾玖万肆仟伍佰柒拾元整)，作为履约保证金。

3、付款方式：

（1）运维服务合同签订后，甲方收到乙方履约保证金和提供的《付款申请单》和等额普通发票后【30】个工作日内，支付总服务费用的【80%】，即人民币￥1556560 元（大写：壹佰伍拾伍万陆仟伍佰陆拾元整）；

（2）本项目运维期满（2025 年 12 月 31 日），且乙方通过甲方运维服务质量考核后，依据最终服务内容审核结果进行支付，支付金额不超过总服务费用的【20%】，即人民币￥389140 元（大写：叁拾捌万玖仟壹佰肆拾元整）。甲方收到乙方提供的《付款申请单》和等额普通发票后【15】个工作日内支付。

（3）运维服务期满（2025 年 12 月 31 日）后进行运维验收，经甲方确认并项目验收合格后，甲方收到乙方提供的《付款申请单》后【15】个工作日内，甲根据运维服务质量考核结论和评分方向乙方无息退回本项目履约保证金，退回金额不超过合同价款的【10】%，即人民币：￥ 194570 元（大写：壹拾玖万肆仟伍佰柒拾元整)

4、甲方收到乙方开具合法等额普通发票后，按照本合同条款约定支付相应款项；因乙方出具的发票存在类型、金额、合法性等问题导致甲方延期付款的，甲方不承担逾期付款的违约责任。

5、在合同履行期间，如遇国家政策调整等因素，导致所开具发票的税率与

上述约定不一致，对应服务费用总额不变，税款金额跟随税率调整。

6、由于乙方未足额缴纳应缴税款和开具发票不真实、不合格而引起的一切责任（包括商业责任和法律责任）和损失，由乙方全部承担。由此给甲方造成的所有损失，乙方还应予全额赔偿。

7、如果乙方根据本合同产生对甲方的赔偿或支付违约金的责任，则甲方有权从最近一笔付款中扣除相应金额。如果最近一笔付款不足以抵扣违约金的，则可从下一笔付款中继续扣除。

8、因项目资金未落实到甲方而引起的甲方延迟付款的情形，甲方不承担逾期付款的违约责任。

9、如甲方支付资金时点恰逢年初拨付，导致支付延迟时，合同款项支付时间顺延。

四、专项条款

（一）服务地点

甲方指定地点。

（二）运行及维护

1.为保障贵州省医疗保障局信息平台能长期安全、可靠、高效运行，乙方至少派驻 3 名驻场技术支持人员，接受甲方工作调度，提供 5*8 小时驻场技术维护服务，随时处理系统使用过程中所产生错误或发现的安全服务问题。

2.服务响应要求：提供 7*24 小时远程网络安全监测及其他相关安全技术服务，保证维护电话通畅。对服务期间的突发安全事件、安全产品使用优化、安全产品故 障等问题提供良好的技术支持和解答，并在 2 小时内予以解决、答复；当进行初步诊断后，依据诊断结论由技术人员通过现场+远程支持进行维护，如确需到现场解决问题，安全运维总部保证技术人员 24 小时内到达，并排除系统故障；重大事项及活动期间需 24 小时提供保障服务。

3.培训要求：按照甲方的运维要求并提供具有相应专业知识、工作和培训经验的人员和相应的教材。培训费用由乙方负责（含场地、教材、师资等），包含

在投标报价内。

4.满足甲方根据实际需求提出的其他服务条款。

（三）运维服务质量考核要求

甲方依据乙方提供的运维内容、操作实施规范性和人员考勤等进行运维服务质量考核，考核不合格甲方有权扣除项目款或项目履约保证金。考核标准为80分合格，考核依据见合同附件4。

1.考核流程

（1）乙方发起验收申请后，甲方根据“考核细则”（附件4）对项目开展全面的考核评估，形成书面的考核结论和评分，并同步提供给乙方。

（2）在书面的考核结论和评分提供给乙方后的7天内，甲乙双方就书面的考核结论和评分进行签字盖章确认。

（3）甲方根据签字盖章确认后的考核结论和评分，作为项目验收、合同付款（扣款）、合同续签的参考依据。

2.成绩运用

在年度考核中:

（1）考核评分80分及以上为考核通过。

（2）大于等于60分并小于80分，扣除履约保证金总金额的【50%】作为违约金。

（3）考核评分小于60分，扣除履约保证金总金额的【100%】作为违约金。

（4）考核中扣除的违约金，在退回履约保证金时直接扣减。

（四）验收标准

1.验收标准依照本项目实施方案、评审报告、项目采购文件、响应文件、《国家电子政务工程建设项目验收大纲》（国家发展和改革委员会令第55号）、及省委省政府关于信息化运维的相关规定执行。

2.整体项目服务期满后，乙方编制项目验收方案，发起验收申请，甲方、或者甲方委托的第三方对相关材料进行形式审查；通过后，甲方或甲方委托的第三方组织相关专家、甲方相关成员成立验收小组召开验收会，给出项目验收意见并签署相关报告。

项目验收不通过，乙方收回相关验收材料，限期完成相关整改后重新提交验收申请。

甲方严格按照国家医疗保障局、贵州省医疗保障局以及贵州省省级政务信息化项目相关验收标准要求对本项目验收。

3.资料移交:本项目通过验收后15个工作日内，乙方须向甲方移交本项目所有资料(包括但不限于:服务总结报告、巡检记录、处理记录、服务考核表等资料)。资料移交纸质版和电子版各一份，纸质资料应为原件，电子版资料应为纸质资料彩色扫描件。

4.乙方需配合甲方完成《贵州省省级政务信息系统项目验收符合性审查及备案细则（试行）》要求的相关审查和备案工作。

五、双方权利与义务

（一）甲方的责任、权利和义务

1、甲方有权随时向乙方了解项目进度，并要求乙方提供项目相关资料。

2、甲方有权对项目资金使用情况进行监督、检查，并要求乙方提供相关资料。

3、乙方调换项目负责人须事先经甲方书面同意。

4、甲方有权按照本合同约定或有关法律法规规定，对本项目进行监督和检查，有权要求乙方按照监督检查情况制定相应措施并对违反法律法规的行为加以整改。甲方不因行使该监督和检查权而承担任何责任，也不因此减轻或免除乙方根据本合同约定或相关法律法规规定应承担的任何义务或责任。

5、甲方有权在乙方履行合同过程中出现损害公共利益、公共安全情形时终止本合同。

6、当甲方发现运维服务人员不按服务合同履行服务职责，或与服务项目的承包人串通给甲方或项目造成损失的，甲方有权要求乙方更换服务人员，并要求乙方承担相应的赔偿责任或连带赔偿责任。

7、甲方在乙方开展运维服务过程中应按合同约定及时向乙方支付款项。

8、甲方应当负责运维项目的所有外部关系的协调，为运维服务工作提供良好的外部条件。

9、甲方应当及时向乙方提供与项目有关的为运维服务工作所需要的项目资料。

10、甲方应当及时对乙方书面提交并要求做出决定的事宜做出书面决定。

11、甲方应当授权一名熟悉项目情况、能在规定时间内做出决定的代表，负责与乙方联系。更换代表，要提前通知乙方。

12、甲方应组织相关部门，对乙方报送的年度运维服务方案在相关政策符合性、可行性、服务内容、服务标准、服务方式、运维管 理规范及投资概算等方面进行评审，并对不符合评审要求的向乙方提出整改要求。

13、乙方出现失职情形，影响本合同继续实施的，甲方有权解除合同。

（二）乙方的责任、权利和义务

1、乙方有权按照本合同约定向甲方收取合同价款。

2、乙方有权自甲方处获得与提供本合同项下服务相关的所有必须的文件、资料。

3、乙方有权要求甲方为乙方履行本合同项下的服务提供必要协助。

4、乙方应接受甲方的监督管理，配合甲方及甲方委托的第三方监理服务单位，并在必要时提交年度运维服务方案要求必须提供的项目相关服务文档。

5、 乙方应对甲方的业务需求充分调研，形成用户需求分析报告，报告需经甲方书面确认。

6、乙方根据甲方确认的需求分析报告，编制年度服务方案，包括运维服务内容、服务标准、服务方式、运维管理规范、服务保障、经费预算等，报送甲方进行汇总。

7、乙方应切实做好服务保障，接受甲方的考核评价

8、乙方应建立安全管理制度和措施，按照《中华人民共和国网络安全法》等法律法规以及政务信息系统安全管理等有关规定实施。

9、乙方应建立健全服务应急处置机制，保障系统日常稳定运行。

10、合同运维期届满后，如下一年度运维采购尚未完成，为保障系统运维平稳过渡，乙方应额外提供一个月的过渡期运维服务。

六、不可抗力

（一）不可抗力的内容包括地震、台风、水灾、战争及其他不能预见的不可抗力事故或因国家法律和政府政策调整致使直接影响本合同的履行或者不能按约定的条件履行的情形。

（二）签约双方任何一方由于不可抗力事件的影响而不能执行合同时，履行合同的期限应予以延长，其延长的期限以双方协商一致的结果为准。但合同价格不得调整。

（三）受阻一方应在不可抗力事件发生后尽快通知对方，并于事件发生后十四天内向对方提供有关部门出具的证明。一旦发生不可抗力事件的影响持续一百二十天以上，双方应通过友好协商，在合理的时间内达成进一步履行合同的合同。

（四）不可抗力发生后，乙方应迅速采取措施，尽力减少损失，并在【24】小时内向甲方代表通报受害情况，按约定的时间向甲方报告损失情况和清理、修复的费用，甲方应对灾害处理提供必要条件。灾害继续发生，乙方应每隔【10】

天向甲方报告一次灾害情况，直到灾害结束。

因灾害发生的费用由双方分别承担：

1、工程本身的损害由甲方承担；

2、人员伤亡由其所属单位负责，并承担相应费用；

3、造成乙方设备、机械的损坏及停工等损失，由乙方承担；

（五）因不可抗力造成的违约，根据不可抗力的影响程度，免除违约方部分或全部应负的违约责任，但法律另有规定的除外。对于本合同的履行，双方协商解决，根据情况决定是否终止本合同。

（六）不论发生何种不可抗力事件，其影响仅限于项目受阻部分，其他未受影响的部分应照常进行。

七、违约责任

（一）违约情形包括但不限于以下内容：

1、未履行或未全面履行项目管理服务合同约定的工作内容；

2、未按约定派驻项目管理人员开展工作；

3、未经甲方同意，更换项目经理及主要项目管理人员；

4、未执行在项目实施过程中与甲方达成一致合同的相关工作；

5、其它经双方确认属于违约的情形；

6、未按要求在验收后 1 个月内提交项目管理文档资料。

针对以上情形，甲方有权追究乙方违约责任，每违约一项，甲方有权追究本项目合同总额的【5%】，同时超过三项或违约引起项目出现重大问题的，甲方可解除合同，且乙方需向甲方支付合同总额 30%的违约金，违约金不足以弥补甲方损失的，乙方需对甲方的实际损失承担全部赔偿责任。

（二）甲方未依照标准条款约定支付项目管理服务报酬的，双方协商解决。

（三）乙方应在工程最终验收结束后一个月内整理与项目管理有关的所有资料并全数移交甲方，如乙方未按时提交甲方所需资料，每延期一天，乙方应按本合同总金额的【1%】向甲方支付违约金，但不应超过本项目合同总额的【5%】。

（四）若乙方未能就项目重大风险提前预警并及时向甲方汇报并提出风险控制措施，导致项目出现严重失控、重要节点无法达成或其他重大损失时，甲方有

权立即终止合同。

（五）失职情形包括但不限于以下内容：

1、项目管理人员消极怠工或出现重大工作失误，导致项目质量严重受损，进度严重滞后，项目总体损失严重；

2、项目管理人员违反保密管理规定，导致敏感信息泄露；

3、违反廉洁从业合同的；

4、其它经双方确认属于失职的情形。

造成严重失职的，甲方有权解除合同，并追究相应责任。

（六）乙方在签订合同时，应同时签署《保密协议》，乙方应严格按照相关规定，落实保密措施，确保合作过程中涉及的国家秘密、业务需求文件、协议、系统设计、技术成果等内容和相关事务的保密安全，未经甲方书面许可，乙方不得向任何第三方提供或透露甲方所有的资料、数据和信息，包括纸质版资料和电子版资料。在本合同期内或合同终止后，未征得甲方同意，不得泄露与本项目、本合同业务活动有关的保密资料。如果乙方或乙方的相关工作人员违反本合同约定的保密义务，乙方应按合同总价的【30%】支付违约金，违约金不足以弥补甲方损失的，乙方应承担相应的赔偿责任。

八、合同争议

（一）双方在执行合同过程中所发生的一切争议，应通过协商方式解决。如协商不成，可向甲方所在地有管辖权的人民法院起诉。

（二）在诉讼期间，除正在进行诉讼的部分外，合同其他部分继续执行。如争议部分严重影响整体合同目的的实现，则应暂停合同执行。

九、合同生效

（一）本合同自双方法定代表人或授权代表签字（或盖章）并加盖公章之日起生效。本合同一式陆份，甲乙双方各执叁份，各份具有同等法律效力。

（二）本合同未尽事宜，双方可另行签订补充合同予以明确，其他形式的变更无效；补充合同与本合同不一致的，以补充合同为准。

（三）本合同受《中华人民共和国民法典》等相关法律法规的保护，未尽事

【本页无正文，为《2025年贵州省医疗保障信息平台建设项目安全运维服务项目采购合同》专属签署页】

甲方：贵州省医疗保障局（盖章）

法定代表人或授权代表（签字）：

日期：2025 年8月 5日

乙方：贵州大数据产业集团有限公司（盖章）

法定代表人或授权代表（签字）：

日期：2025年7月31日

宜，均按《中华人民共和国民法典》等相关法律法规的规定执行。

十、合同附件

（一）保密合同书

（二）廉政共建合作合同

（三）分项清单

（四）服务考核表

【本页以下无正文】

附件1：保密合同

保密合同

甲方：贵州省医疗保障局

乙方：贵州大数据产业集团有限公司

为确保甲乙双方顺利进行项目的合作，确保项目建设中涉及的相关信息的保密安全，经协商一致，针对合作过程中涉及到的相关信息，甲乙双方达成如下合同并承诺共同遵守：

一、信息保密的范围

本保密合同所指“信息”包括任何以口头、书面、图表或电子形式存在的以下内容：

1. 任何涉及甲方过去、现在或将来的人员结构、规章制度、质量体系、工作流程、处理手段、财务等信息；

2. 任何甲乙双方在项目建设中涉及的技术措施、技术方案、软件应用与开发，以及硬件设备的品种、质量、数量、品牌等；

3. 任何甲乙双方在项目中涉及的技术秘密或专有知识、文件、报告、数据、软件、流程图、数据库、发明、知识秘密，无论上述信息是否享有知识产权；

4. 任何甲方其它的以有形方式或无形方式存在的且不被社会公众知悉的信息。

这些“信息”无论乙方何时接受或接触到，均属保密信息。

二、甲乙双方的保密义务

1. 对不再需要保密或者已经公开的技术信息和技术资料，甲方应及时通知乙方。

2. 乙方对于从甲方处收到的信息，在未经甲方事先书面许可的情况下，不得以任何方式提供给项目之外的第三方及双方的无关人员。

3. 乙方对于从甲方处得到的信息，应当通过建立内部保密制度、培训工作人员保密意识等方式和措施，确保信息的安全。

4. 乙方承诺，所收到的甲方信息只能用于项目而不得用于任何其他目的。

5. 乙方承诺，所收到的甲方信息在本方此项目工作组中能得到谨慎的使用，只能用于本方参与此项目的相关人员，并且保证该相关人员在知晓信息之前已经充分了解了本合同的内容。

6. 乙方承诺，对于所收到的甲方信息，未经甲方事先书面许可，不得以任何形式复制和传播。

7. 除甲方事先书面同意，否则乙方不得向第三方以任何形式透露双方的任何会谈、会议、协商或共同工作的内容。

8. 除双方另有约定外，负有本合同约定的保密义务的主体包括：乙方参与或曾经参与项目的人员、以及在工作中有意或无意获悉本合同约定的保密信息的其它人员（包括但不限于乙方的工作人员）。

9. 乙方因为建设项目目的，从甲方处取得的书面或电子信息，应当在项目完成后即时完整归还甲方。

10. 乙方利用自有设备或甲方设备在软件开发调试及设备配置过程中，杜绝发生“一机两用”等违反网络信息安全规定的行为。

11. 除非双方书面同意，本合同所规定的保密期限为永久。

12. 甲方提供信息的行为不得被视为是以任何方式授予技术许可，或是转让著作权、商标权、专利权或技术秘密的行为。取得甲方信息，并不表明取得了信息的任何知识产权；甲方所提供的任何信息的知识产权和财产权利，全部归甲方所有。

13. 如乙方工作人员因完成项目需要进入甲方工作场所，应当严格按照甲方的相关规章制度，不得进入甲方未授权进入的办公区域，不得在与项目工作无关的区域活动。

三、其他约定

鉴于甲乙双方形成的合作关系，本合同约定的保密义务作为乙方向甲方履行生产、供货义务的附随义务，甲方不再另行支付乙方保密费用，乙方不得以任何理由及任何方式以本合同为依据向甲方主张权利。

四、违约责任

若一方违反上述任条款，给对方造成损失的，由违约方承担相应责任，并赔

偿由此产生的损失。双方违反规定的，各自承担应负责任，直至追究法律责任。

【以下无正文，为《保密合同》签署信息。】

甲方：贵州省医疗保障局（盖章）

乙方：贵州大数据产业集团有限公司

（盖章）

甲方代表签字：

乙方代表签字：

签字日期：2025年8月5日

签字日期：2025 年 7 月 31 日

附件2：廉洁共建合作合同

廉洁共建合作合同

甲方：贵州省医疗保障局

乙方：贵州大数据产业集团有限公司

为维护甲乙双方的合法权益，健全和完善监督制约机制，预防职务犯罪行为的发生，保证双方企业依法经营、业务工作人员廉洁从业，根据国家有关法律法规的规定，经双方自愿、平等协商，特签订如下廉洁共建合作合同。

一、双方应在遵守国家政策、法规的前提下开展业务交往活动，不得违法经营。充分尊重并配合执行对方有关廉政建设的各项制度及规定。

二、在业务交往活动中，应贯彻平等、互利、公平、协商一致的原则，自觉履行经济合同。

三、双方业务工作人员要廉洁勤政、秉公办事，提高服务质量，讲究工作效率，不扯皮推诿，不刁难对方。

四、双方发生经济往来，必须通过银行结算。业务往来中有关优惠、让利必须写入合同，放在明处，不得以任何理由或方式截留。

五、双方业务工作人员不得擅自发生任何形式的借款、租赁及财产买卖关系。

六、双方业务工作人员不得以任何理由、方式向对方索要或赠送现金、有价证券、支付凭证和高档贵重礼品，以及各种名义的回扣、好处费、感谢费等。不得到对方报销应由本方个人或集体支付的各种费用。

七、双方业务工作人员不得利用婚丧、乔迁、升学等名义，向对方单位或个人收取或赠送钱财。

八、双方业务工作人员不得利用职权卡扣应付款项；不得利用职权以威胁恐吓、不配合等方式干扰合作方的正常工作；不得利用职权以隐瞒包庇、不作为等方式纵容合作方违规操作；不得与第三人恶意串通，以包含但不限于串标、围标、泄露标底、虚报价格、制定虚假方案、虚增工程量、虚办签证、供应伪劣残次材料、设备等方式，损害合作方的合法利益。

九、双方业务工作人员不得以职权和职务影响或工作便利违规为本方或对方亲朋好友牟利。

十、双方在业务交往中需要招待的，要本着必要、适度、从俭的原则，不得铺张浪费，不得组织、参加不健康的活动和高消费娱乐活动。

十一、双方业务工作人员不得向对方或第三方泄露经济秘密。

十二、双方有义务配合对方反馈本合同的执行情况并及时向对方通报本单位的廉洁规定，在交流业务的同时要交流廉洁建设的经验，互相监督，共同提高。

十三、双方应自觉履行本合同的各项规定。甲方业务工作人员违反上述有关规定，乙方可向甲方负责人通报，也可以向甲方投诉、举报，甲方将及时向乙方通报查处情况。乙方违反上述有关规定，甲方应向乙方负责人通报，并视情节轻重，按照警告、取消投标资格、取消合格乙方资格及列入黑名单的方式减少或停止与乙方的业务往来，后果由乙方负责。

【以下无正文，为《廉洁共建合作合同》签署信息。】

甲方：贵州省医疗保障局（盖章）

甲方代表签字：

举报电话：

举报邮箱：

签字日期：2025年8月5日

乙方：贵州大数据产业集团有限公司（盖章）

乙方代表签字：

举报电话：

举报邮箱：无

签字日期：2025 年 7 月 31 日

附件3：分项清单及价格表

服务内容	服务分项	税率	价格（元）
日常安全运维	资产发现服务	6%	96500
	安全监测服务	6%	96500
	安全预警服务	6%	96500
	安全分析服务	6%	135100
	取证溯源服务	6%	135100
	应急响应服务	6%	134100
	安全事件处理服务	6%	134100
	安全加固和策略优化服务	6%	96500
专项安全运维	业务系统安全基线	6%	88000
	安全建设管理	6%	88000
重大活动保障	重大活动保障	6%	310000
渗透测试专项	渗透测试专项	6%	220700
攻防演练	攻防演练	6%	160000
安全培训服务	安全培训服务	6%	20000

机关大楼安全运维	机关大楼安全运维	6%	77000
APP安全加固	APP安全加固	6%	57600
总价			1945700

附件4：服务考核表

服务考核表

考核指标	默认分值	评分标准	评分
交付物质量	10	按照《项目运维服务管理规范》和合同各项运维要求，完成 各个阶段文档交付工作，且文档被甲方及最终用户认可。 1. 交付物提交不及时，每次扣1分。 2. 交付物质量不合格，每次扣2分。 3.每缺失一个阶段的文档交付物，每次扣5分。	

		4.交付物提交不及时，并且质量不合格，且发生两次及以上， 每次扣5分。	
日常巡检	5	按照合同和采购文件要求对安全产品进行例行巡检。 1.未按上述要求开展相关工作的，每出现一次扣1分。 2.因未进行日常检查，或因检查不彻底、发现隐患不及时， 最终导致系统出现故障的情况，每出现一次扣5分。	
运维服务	30	运维服务要符合《项目运维服务管理规范》和合同各项运维 要求，提供的运维服务需要获得甲方及最终用户的认可。 1.未按照《项目运维服务管理规范》和合同各项运维要求开 展工作，导致不良影响的，每次扣2分；造成严重后果的， 每次扣10分。造成特别严重后果的，每次扣20分。 2.运维服务过程中，受到甲方及最终用户的投诉电话，每次 扣20分。 3.乙方单位在运维服务过程中受到甲方及最终用户的书面表扬的，每次加10分。	
应急响应和故障处置	20	要符合《项目运维服务管理规范》和合同各项运维要求，对 系统和服务出现的紧急情况及时响应并妥善处理，处理情况 及时反馈甲方及最终用户。 1.出现紧急情况，在10分钟内未响应，每次扣1分；在30分钟内未响应，每次扣5分；1小时内未响应，	

		每次扣10分；1小时以上未响应，每次扣20分。 2.因乙方单位原因，造成系统(或关键功能)大范围中断、 系统访问缓慢(响应时间在30秒以上),大量用户无法正常开展工作的情况，故障时间在10分钟以内，每次扣5分；30 分钟以内，每次扣10分；1小时以内，每次扣20分，每增加 1小时加扣10分。 3. 日常故障处理之前，没有征得甲方及最终用户的同意，私 自进行运维操作的，每次扣20分。 4.针对与乙方服务范围内无关的突发情况，乙方及时配合甲方及最终用户，起到决定性的作用并妥善处理，使甲方及最 终用户的损失降到最小，每次加10分。	
沟通、协调	5	与本单位运维团队紧密衔接工作，并能与甲方及最终用户、其他项目运维单位保持良好沟通和协作。 1.不能有序、有效开展上述协作的，影响项目进展情况的， 每次扣1分。 2.沟通协调过程中态度恶劣，没有责任心的，每次扣2分。 3.沟通协调过程中出现谩骂、不尊重人的，每次	

		扣5分。	
工作态度	5	根据甲方及最终用户的要求完成项目范围内交办的有关工 作。 1.能够完成交办的工作，但完成的及时性、准确性方面存在 不足，每次扣1分。 2.针对甲方及最终用户交办工作，30分钟内没有积极响应的， 每次扣2分。 3.不接受、不配合交办的工作，每次扣5分。	
重大活动及节假日保障工作	20	重大活动及节假日保障工作是指在重大活动或者特殊时期进 行运维和安全保障，无任何安全事件发生。 1.因保障力度不够，没有造成安全事件发生，但是产生不良 影响的，每次扣10分； 2.因保障力度不够，造成安全事件发生的，每次扣20分。	
工作评价	5	对项目范围内的各项工作开展情况随机进行2~3次的评价， 由甲方及最终用户评价。 1.评价为一般，每次扣1分。 2.评价为不满意，每次扣2分。	

		3.评价为极度不满意，每次扣5分。	
合计			

注：出现重大网络安全事故，被省级及以上部门通报，扣100分。

建设单位	我方已按照合同要求完成相关服务内容，现正式提请服务考核。 建设单位（盖章）： 项目负责人： 日期：
用户单位	用户意见： 用户单位（盖章）： 用户单位代表： 日期：