

一、项目名称

巴彦淖尔市医院智慧医疗大数据服务项目

二、项目概况及目的

本项目旨在为医院构建安全可靠、高效敏捷、统一管控的 IT 基础架构，通过采购云服务器、裸金属服务器及存储、网络专线、云服务统一管控平台等关键技术服务，全面提升医院信息化支撑能力。项目最终目标是保障医院信息系统的安全、稳定、高效运行，确保医疗业务的连续性和数据的安全性，满足未来业务扩展和技术升级需求，为医院智慧医疗和大数据应用提供坚实可靠的 IT 基础保障。

三、采购内容

(1) 采购清单

响应人需在投标文件中写明详细的报价清单，清单需包含但不限于以下内容：

序号	采购内容	详细要求	备注
1	云服务器及存储服务	见具体要求	
2	裸金属服务器及存储服务	见具体要求	
3	网络专线服务	见具体要求	
4	云服务统一管控平台服务	见具体要求	
5	其他相关服务要求	见具体要求	

备注：投标人应按报价要求进行细化

(2) 服务期限

自合同签订之日后 15 日内交付验收完成，验收合格之日起服务期 3 年。

(3) 报价要求

- 1、投标人应全面评估本项目实施所需的各项资源与服务，若其认为采购清单中存在遗漏或不足以实现项目目标的，应在投标文件中予以补充，相关费用视为已包含在总报价中，中标后不得以漏项为由追加费用。
- 2、★项目涉及的任何和项目运行相关的服务费用（包含不限于信息系统完整迁移、资源总量临时调整、云平台相关软硬件升级等）均包含在响应人响应报价内不另行收费。投标人需在投标文件附件中列出详细报价清单，例如系统迁移费用，需列出系统迁移费用价格。（备注：1、提供承诺函（格式自拟）并加盖响应人

公章，承诺满足上述要求。2 响应人需在投标文件附件中列出详细报价清单。)

四、详细参数及相关要求

1、响应人提供的技术方案，必须满足以下原则：

(1) 先进性原则

云平台必须严格遵循国际标准、国家标准和国内通信行业的规范要求同时满足后续升级的需求。

(2) 高可靠性

云平台稳定可靠性是业务运行的基础，影响着企业日常办公、业务的发展。系统的可靠性包括整体可靠性、数据可靠性和单一设备可靠性三个方面。云平台架构合理，从整体系统上提高可靠性，降低系统对单设备可靠性的要求。系统的可用性是通过冗余、高可用集群、应用与底层设备松耦合等特性来体现，从硬件设备冗余、链路冗余、应用容错等方面充分保证整体系统的可用性。

(3) 可扩展性

根据医院业务不断发展，云平台也会不断地扩充变化，要求在保证云平台安全的基础上具有灵活的、平滑可扩展性。

支撑云平台的资源需要根据业务应用工作负荷需求进行弹性伸缩，IT 基础架构应与业务系统松耦合，这样，在业务系统进行容量扩展时，只需增加相应数量的 IT 硬件设备，即可实现系统的灵活扩展。

(4) 开放兼容性

云平台的安全产品设计规范、技术指标符合国际和工业标准，支持多厂家产品，从而有效地保护投资。

(5) 安全最小授权原则

云平台的安全策略管理必须遵从最小授权原则，即不同安全区域内的主机只能访问属于相应区域资源，对云平台资源必须完全得到控制保护，防止未授权访问，保证云平台的信息安全。

具体要求如下：

序号	类型	项目	要求
1	服务器	裸金属服务器	使用国内通用主流服务器品牌、型号
2			采用最新稳定硬件型号、版本

序号	类型	项目	要求
3		虚拟服务器	支持 SNMP 监控协议、并接入监控平台
4			使用国内通用主流虚拟化平台软件产品
5			采用成熟稳定、在行业内已规模应用的硬件型号和版本
6			支持 SNMP 监控协议、并接入监控平台
7	存储	存储设备	使用国内通用主流存储器品牌、型号
8			存储设备所涉及的核心交换机、业务接入交换机、管理接入交换机等重要设备需要支持冗余备份；
9			具备存储虚拟化功能
10			支持 SNMP 监控协议、并接入监控平台
11			具备 web 页面提供配置和监控
12	网络	网络设备	全网络节点具备双机，避免单点故障
13			所有网络设备具备被监控能力，如支持 SNMP 协议
14	安全	安全设备	安全设备及组成架构满足每年国家最新等保 2.0 三级要求，并出具相关测评证书。
15			具备网络边界安全防护设备。对勒索病毒及其变种病毒有针对性保护。
16	链路	网络链路	提供满足业务需要的 4 条或以上高带宽点对点专线，具备双链路冗余和负载机制。
17	备份	系统备份	物理机做主备、群集功能实现高可用
18			虚拟化使用 HA 高可用功能
19			使用备份软件、如备份软件实现系统级备份
20		数据库备份	主库做主备、双机，并使用数据库灾备软件做容灾
21		应用备份	应用做集群、负载，并使用专业应用、文件灾备软件做容灾
22		冷备	定期每日增量备份，每周全备，备份存放多份，具体详见备份细则

序号	类型	项目	要求
23		恢复时间	关键业务系统按约定恢复时间目标执行，具体以备份策略为准。
24	系统 数据库	数据库	提供采购人所需的 Microsoft SQL Server 企业版、ORACLE（50 用户）等正版数据库。
25		操作系统	提供采购人所需的正版操作系统
26	服务	升级服务	云服务统一管控平台相关软硬件的部署、运行及升级服务。
27		部署服务	根据采购人实际需求提供对云资源和网络配置适配服务。协助完成信息系统的部署。（资源具体使用根据采购人实际使用要求进行服务器分配及操作系统和数据库的部署。）
28		安全服务	提供所租赁云资源上承载的所有虚拟机的系统部署、升级、安全漏洞扫描及补丁安装等配套服务；
29		迁移服务	中标人完成本项目云资源上部署的所有虚拟机、数据库、数据的迁移工作。
30		备份服务	提供所有虚拟机承载信息系统的容灾备份（含数据库）。保障所租赁资源上承载的所有业务的正常运行及应急响应和处置工作。
31		保障服务	提供云数据中心机房建设和安全运行，满足采购人的网络数据安全、系统稳定、24 小时不间断运行的高性能要求。
32		专线服务	提供项目涉及的云平台 and 专线的运行维护，提供高质量运行维护服务。
33		协调服务	负责与本项目云平台有关的其他三方公司的协调工作。
34		保障服务	提供本项目涉及云服务的维护服务，包括本次项目提供的云服务资源以及云管平台所涉及软硬件故障处理、定期设备健康检查、完整的系统规划

序号	类型	项目	要求
			及风险评估、系统软硬件升级、系统 BUG 修复、云管平台更新调整、微码升级、根据实际需要进行扩容服务等；全面保证所含云服务资源的持续安全稳定运行。

★2、资源配置要求

2.1 供应商应确保所提供的资源以独立私有云形式提供，不得与其他云池共用。

2.2 供应商所提供的云服务器及存储资源、裸金属服务器及存储资源不得低于本文件“3.1 云服务器及存储资源要求”和“3.2 裸金属服务器及存储资源要求”中列明的配置和数量。

2.3 供应商应确保所提供资源的性能和容量能够支持采购人信息系统的稳定、流畅运行。在系统部署及试运行期间，如因资源不足或配置不当导致系统性能不满足业务需要，供应商应在不增加采购人额外费用的前提下，负责对资源配置进行优化或扩充，直至系统正常运行。

（备注：响应人提供承诺函（格式自拟）满足上述要求并提供详细的资源配置清单，加盖供应商公章。）

3、服务器及存储资源要求

3.1 云服务器及存储资源要求

类型	云资源内容		
云资源	VCPU	内存	容量型存储容量
	4520 核	8800G	347.2T

3.2 裸金属服务器及存储资源要求

序号	类型	参数	数量	备注
1	服务器 1	CPU: 2.2Ghz 2*10 核 20 线程、内存 128G、不低于 480GB SSD ×3、双电源	4 台	

2	服务器 2	CPU: 2.3 Ghz 2*12 核 24 线程、内存 256G、不低于 1.2T SAS ×2、双口万兆网卡（含多模模块）、双电源	2 台	
3	服务器 3	CPU: 2.2 Ghz 2*12 核 24 线程、内存 256G、不低于 480G SSD x3、双口万兆网卡（含多模模块）、双电源）	2 台	
4	服务器 4	CPU: 2.3 Ghz 2*12 核 24 线程、内存 256G、不低于 1.2T SAS ×2、双口万兆网卡（含多模模块）、双电源）	2 台	
5	服务器 5	CPU: 2.3 Ghz 2*12 核 24 线程、内存 256G、不低于 480GB SSD ×3、双口万兆网卡（含多模模块）、双电源	2 台	
6	数据库存储	提供可用资源 19.8T 高性能的块存储，采用全 SSD 存储介质，满足 NoSQL/关系型数据库高 IO 和低延迟要求，适用于高性能、高读写速率要求，以及数据密集型应用场景。	1 套	
7	负载均衡	2 个万兆光口口，6 个千兆电口；双电源，热插拔；4 核处理器，内存 8GB；吞吐默认 6G，可扩展至 12G，最高可升级至 26G；支持虚拟化，实现重要业务隔离，默认送两个 vadc，可升级至 24 个 VADC；支持 SSL 卸载；应用分发支持 3 层到 7 层均支持；4 层每秒 7000K CPS，7 层每秒 900K RPS，最高并发 session 1200W；	3 台	
8	网络服务	核心交换机、业务接入交换机、管理接入交换机等重要设备需要支持冗余备份；	一套	

★ 4、网络数据专线要求

提供满足业务需要的 4 条或以上不同路由的高带宽点对点专线，具备双链路冗余和负载机制，单条专线带宽不低于 10GE。（备注：提供承诺函（格式自拟）

并加盖响应人公章。)

5、云服务统一管控平台要求

5.1 提供云服务统一管控平台一套，响应人需要在投标文件中对云管控平台进行详细功能描述（要求提供系统截图），要求包含以下基本功能或相似功能，现有系统若无以下基本功能，需明确的写出解决方案、措施、实施方法。响应人承诺根据医院实际使用需求免费升级云管控平台。

5.2 云管控平台基本功能要求：

序号	功能描述
▲1	1 支持 UnderLay (VLAN) 类型的网络，支持基于云原生的 Kube-ovn 技术架构的网络能力，提供不同的网络服务：包括 VLAN 网络、子网、网络 ACL、安全组、虚拟网卡、HA VIP 等功能【提供界面截图】。
2	云管控制平台能够提供虚拟机服务，用户通过自助服务门户申请所需操作系统、CPU 核数、内存、硬盘以及相应网络 IP，云管理员也可以将已存在的虚拟机指定给某一个用户。【提供界面截图】
▲3	用户在申请虚拟机时，可以为虚拟机选择自定义密码或者选择随机密码。【提供界面截图】
▲4	支持用户采用加密方式登录云主机，保证用户登录安全。【提供界面截图】
▲5	创建子网可指定内网网段、VLAN 号、网关等信息，子网可查看内网 IP 使用情况。支持按需设定子网中的预留 IP，预留 IP 不会自动分配给云主机。【提供界面截图】
6	裸金属需支持手动和自动挂载云盘两种方式。 在具备块存储资源时，提供挂载云硬盘能力。不具备块存储资源是支持屏蔽挂载能力。 手动挂载场景，控制台提供 iscsi 命令挂载指引。【提供界面截图】
▲7	支持对计算节点的 CPU、内存、存储容量和虚拟化平台相关存储卷的存储容量进行统计展示及阈值告警设置，当监控到实际资源使用达到设定阈值时发出告警通知。【提供界面截图】
▲8	云平台控制台支持部署在本地、在本地进行访问、独立管理，非绕行到

	其他云站点中进行控制台访问。【提供界面截图】
▲9	云管控平台管理节点须支持 Docker 集群部署，并支持部署在物理机上，提供平滑升级扩展、高可靠容错机制。【提供界面截图】
▲10	支持提供展示云主机、云存储、对象存储、云网络等各项云服务资源的资源利用率、资源使用数量、性能指标的视图；【提供界面截图】
▲11	虚拟机可以实现物理机的功能，如具有自己的资源（内存、CPU、网卡、存储），可以通过控制台指定单独的 IP 地址；【提供界面截图】
12	云硬盘支持配置自定义大小的系统盘、数据盘；【提供界面截图】
13	支持 IPv4、IPv6、双栈网络能力；【提供界面截图】
▲14	支持虚拟机、容器，可直接将虚拟机和容器调度至同一个云网络，实现云主机与容器的二层互通

6、服务要求

6.1 实施要求

序号	服务要求
★1	响应人应提供详细可执行的系统迁移实施方案。方案要求确保迁移过程中云上所有业务的连续运行（业务不中断）和迁移后数据的完整性。响应人需承诺如在迁移过程中因业务中断或数据损坏等造成任何的损失由其完全负责。（备注：提供详细的系统迁移实施方案，并附承诺函（格式自拟），承诺对迁移过程中的损失承担全部责任；方案需包含迁移步骤、应急预案、业务连续性保障措施等。上述材料均需加盖响应人公章。）
2	响应人应保证所提供的系统完全符合规定的功能和性能要求。响应人应对由于设计的技术缺陷而产生的故障负完全责任。
3	响应人提供的产品必须包括投标产品便于应用集成开发的组件和套件、设计开发工具、服务监控、技术文档及全部功能模块的售后服务等，其所提供的所有功能模块、组件和套件等使用权必须为业主方，且必须是最终用户业主方的正规产品。业务培训包含所有功能模块的知识内容。响应人不得为应标遗漏或省略某些功能模块。

★6.2 安全要求

为保障医疗数据安全、满足应急响应及时性及监管便利性要求，本次投标中涉及的云资源机房所在地必须为招标人所在地区。该项目中所采购内容（包括但不限于云资源、服务器、网络设备、安全设备、专线、服务及机房等物理环境等）均需在采购人所在地区（城市）提供。（备注：响应人需提供承诺函（格式自拟）并加盖响应人公章，承诺满足上述要求。）

响应人需要在投标文件中写明网络安全服务方案，包括但不限于机房环境、网络安全、链路传输保证、系统容灾等方案。机房应通过国家云机房信息安全三级保护测评并提供公安机关认证的网络安全等级保护测评证书。

（备注：提供详细的网络安全服务方案，方案内容需涵盖机房环境、网络安全、链路传输保证、系统容灾等方面；提供该项目所涉及物理环境在有效期内的公安机关认证的网络安全等级保护测评证书；上述材料均需加盖响应人公章）

6.3 云资源部署要求

派遣专业技术人员依据采购人业务需求进行云资源部署、调整和相关配置变更。要求如下：

序号	服务内容	响应时限（小时）
1	云主机开通	4
2	云主机删除	4
3	云主机变更	影响业务，需要与甲方约定调整时间窗口，在调整时间窗口时间段内完成
4	存储新增	
5	存储削减	
6	存储扩容	
7	网络变更	4
8	端口开通	2

6.4 备份服务要求

序号	服务类型	服务要求
★1	数据库备份	通过如数据库自带工具、数据库备份工具等，对数据文件、日志文件进行备份。要求每天进行增量备份，每周进行全量备份。所备份数据需进行多份存储。定期对备份状态进行巡检并配合招标人进行业务切换测试。（备注：投标人需提供满足该项目的备份工具的照片、运行界面截图及授权证明；投标人需提供提供详细的数据库备份方案，方案中需明确备份工具、备份周期、备份存储方式及巡检机制；提供承诺函（格式自拟），承诺在服务期内所提供的备份工具的可靠性、稳定性、安全性及授权持续性；承诺按照上述技术要求实施备份策略并配合业务切换测试。以上材料均需加盖响应人公章。）
2	应用备份	通过如应用备份工具等，对应用程序文件、数据文件进行备份。要求每次升级后进行备份，每周进行全量备份。所备份内容需进行多份存储。定期对备份状态进行巡检并配合招标人进行业务切换测试。
3	备份验证	<p>（1）备份工作完成后，立即对备份数据在验证环境、测试环境进行验证，确保备份数据准确、有效，并写入巡检报告；</p> <p>（2）值班人员必须认真执行巡检制度，发现问题及时反馈相应人员；</p> <p>（3）系统数据备份后，需配合院方进行数据验证，在验证环境下对数据有效性进行验证应定时检查备份文件中是否存在备份失败的记录，如发现有备份任务失败的记录，需要检查故障原因，并进行排除。缺乏何时进行验证及验证频率的要求。每季度至少配合院方进行开展一次全量备份数据的恢复验证演练，每次验证须覆盖核心业务模块，并记录验证过程与结果；针对关键系统，需配合院方进行每月一次增量备份验证。需配合院方进行验证，完成后 24 小时内提交验证报告，经运维负责人签字确认</p>

		后归档。
--	--	------

6.5 巡检服务要求

序号	类型	内容	记录	备注
1	值班	<p>(1) 机房实时全天 24 小时值班责任制，值班人员必须遵守值班和交接班制度；</p> <p>(2) 按规定执行现场维护作业计划，及时准确、完整地填写值班交接班日志及各种规定的记录。</p>	所有巡检、交接班信息，全部记录到巡检报告和交接班记录本供医院检查	
2	例行巡检	<p>(1) 机房巡检人员执行每天巡检 2 次，并准确记录设备运行健康状况，包括服务器、网络、电力、空调等；</p> <p>(2) 系统巡检人员执行每天巡检 2 次，并准确记录操作系统健康状态，网络状态，网络安全状态，统计每日操作。</p>		
3	突发巡检	突发巡检主要针对抽查业务的运行质量指标采集的真实性和准确性，印证业务真实的运行质量。		
4	交接班	<p>(1) 交接班内容包括设备运行状况、障碍情况，备品备件、文件资料、工具仪表，相关业务通知，上级批示以及需由接班人继续处理的问题；</p> <p>(2) 交接班人员应将交接内容逐项检查核实并确认无误，在值班交接班日志上签字后，交班人方可离岗；</p> <p>(3) 交接班过程中发生障碍或事故，应暂停交接，以交班人员为主，接班人协助共同处理，直至障碍或事故消除，或处理告一段落后</p>		

		再继续交接； (4) 因漏交或错交产生的问题，由交班人员承担责任；因漏接或错接而产生的问题，由接班人承担责任；交接双方均未发现的问题，由双方承担责任。		
--	--	--	--	--

6.6 运维保障要求

序号	维护内容	周期
1	登陆监控软件查看端口告警情况，异常时告警通知记录	4 小时一次
2	登陆监控软件查看主机连接数情况，异常时告警通知记录	4 小时一次
3	登陆监控软件查看接口输出带宽利用率，异常时告警通知记录	4 小时一次
4	登陆监控软件查看设备响应时间，异常时告警通知记录	4 小时一次
5	登陆监控软件查看接口发送速率，异常时告警通知记录	4 小时一次
6	查看核心交换机 log 日志，异常时告警通知记录	4 小时一次
7	登录查看云主机 CPU 使用率，异常时告警通知记录	4 小时一次
8	登录查看云主机内存使用率，异常时告警通知记录	4 小时一次
9	登录查看云主机网络吞吐量，异常时告警通知记录	4 小时一次
10	登录查看管理平台的告警日志，异常时告警通知记录	4 小时一次
11	整理故障报告	每天一次
12	更新云计算资源汇总表，资源告警时记录及通知	每天一次
13	整理设备端口使用情况，端口通讯异常时处理记录及通知	每周一次
14	查看虚拟机、物理机的数据备份状态，异常时处理记录及通知	每天一次
15	整理设备地址使用情况，异常时告警通知记录	每周一次
16	整理 VLAN 使用情况，异常时告警通知记录	每周一次
17	整理 ACL 情况，异常时告警通知记录	每周一次
18	收集 ARP 情况，异常时告警通知记录	每周一次

19	系统运行质量情况、障碍情况统计分析	每月一次
20	系统操作权限及口令的验证、修改	每季一次
21	网络安全状态检查，统计各安全设备安全报警情况	每天一次
22	漏洞扫描，对网络接入设备（交换机、路由器等）、网络安全设备（防火墙等）、主机服务器的操作系统、数据库、应用服务器提供扫描结果	每月一次

7、应急响应要求

★7.1 应急响应总体要求

投标人应建立完善的应急响应机制，配置专人提供 **7×24 小时** 应急支持服务，针对系统运行异常、突发故障及紧急技术支持请求，能够快速响应、分级处理、有效恢复，最大限度保障业务系统连续、稳定运行。要求所有故障响应时间不得超过 4 小时，恢复云平台运行不得超过 24 小时。

投标人应结合本项目实际情况，制定专属应急预案，并在故障时按本章规定流程执行。（备注：提供应急响应方案及专属应急预案，包含应急组织架构、响应流程、故障分级、处理时限、保障措施等内容；提供承诺函（格式自拟），承诺满足 7×24 小时应急支持及故障响应恢复时间要求。上述材料均需加盖响应人公章。）

7.2 应急响应服务内容

序号	类型	内容
1	故障发生	当系统发生异常或故障时，投标人应通过监控系统告警、人工发现或采购人反馈等方式第一时间确认故障情况；应第一时间（原则上不超过 10 分钟）及时通知采购人，并说明故障现象、影响范围及初步判断。
2	故障分级与升级	投标人应按照故障对业务系统影响程度，对故障进行分级管理（I 级—IV 级），具体分级标准及响应要求详见 2.4 服务等级与响应时间；在故障处理过程中，如故障影响范围扩大、持续时

		间延长或达到更高级别故障标准的，应自动升级故障级别，并同步启动对应级别的应急处理程序；故障升级情况应及时告知采购人。
3	故障处理与信息通报	故障处理期间，投标人应持续向采购人通报处理进展情况；对于 I 级故障，应在关键处理节点向采购人反馈处置情况；对于 II 级及以上级别故障，应每 30 分钟向采购人通报一次处理进展，直至故障恢复或进入应急保障状态；在故障处理过程中，投标人应采取必要措施，最大限度保障数据安全，防止数据丢失或进一步损坏。
4	应急预案启动与保障措施	当评估故障在约定处理时限内无法恢复，或可能对业务系统连续运行造成严重影响时，投标人应立即向采购人申请启动应急预案；经采购人同意后，投标人应按照应急预案要求，及时启动备份系统、容灾机制或其他应急保障措施，确保业务系统的基本运行；应急处置期间，投标人应持续跟踪系统运行状态，并配合采购人开展相关协调工作。
5	故障恢复与总结整改	故障排除后，投标人应在 24 小时内向采购人提交故障处理记录或书面报告；报告内容应包括但不限于：故障现象及影响范围、故障原因分析、故障处理过程及采取的措施、数据及业务恢复情况。 投标人应根据故障情况提出合理的整改建议，并在合同服务范围内协助采购人完成整改，防止类似问题再次发生。

7.3 故障服务等级与响应时间

故障等级	响应时限要求	故障恢复时限
I 级故障	10 分钟	2 小时
II 级故障	10 分钟	4 小时

III 级故障	10 分钟	6 小时
IV 级故障	10 分钟	8 小时

8、技术文档

序号	资料类型	内容
1	架构图	数据中心硬件架构图、硬件拓扑图
2	配置资料	(1) 服务器硬件 BOIS、RAID 等配置资料 (2) 操作系统版本、补丁、分区、性能级别等配置资料 (3) 安全设备、软件策略配置资料 (4) 网络设备配置资料
3	维护手册	机房保障手册
4	系统日志	提供云管理平台的日志
5	修改记录	修改记录文档提供日后核查
6	故障处理记录	故障处理记录文档提供日后核查。
7	值班日志	值班日志记录
8	通讯录	应标人相关人员通讯录

9、其他服务要求及其他说明事项

1. 其他要求

1.1 服务保证承诺要求

招标文件中要求投标人进行承诺的内容,需要在投标文件中提供正式的服务保证承诺书,承诺内容符合招标文件要求,服务保证承诺书视为合同中组成部分。

2、付款阶段及比例

2.1 付款阶段及比例

分三年支付:

年度	付款时间	付款比例	付款条件
----	------	------	------

第一年	达到付款条件后 90 日内	合同金额的 30%	1. 合同正式签订生效； 2. 供应商提供等额正规合规发票（增值税专用发票）。
	达到付款条件后 90 日内	合同金额的 30%	1. 供应商提交项目交付验收报告，并经采购人验收合格； 2. 供应商提供等额正规合规发票（增值税专用发票）。
第二年	达到付款条件后 90 日内	合同金额的 20%	供应商提交第一和第二年度项目服务验收报告，并经采购人验收合格； 2. 第一和第二年度服务期内无重大违约记录，或已完成整改； 3. 供应商提供等额正规合规发票。
第三年	达到付款条件后 90 日内	合同金额的 20%	1. 供应商提交第三年度项目服务验收报告，并经采购人验收合格； 2. 第三年度服务期内无重大违约记录，或已完成整改； 3. 供应商提供等额正规合规发票。

2.2 其他付款说明

若因供应商原因导致未能按时完成服务或未能达到验收标准，采购方有权暂停支付剩余款项，直至供应商采取有效措施解决问题并重新完成服务周期且验收合格后，再按照本付款方式的约定支付剩余款项。

3、验收相关事项

3.1 履约验收内容

3.1.1 交付产品及服务：对照招标文件及中标人投标文件，核查所提供软硬件产品的品牌、型号、规格、数量、技术参数是否一致，确保所有软硬件及系统均为原厂正品且符合采购人要求。

3.1.2 功能性能验证：中标人所提供的云平台、裸金属服务器、存储、网络及安全设备等可通过功能测试和性能验证，确保满足招标文件中规定的各项技术指标

（如符合行业通用接口标准、稳定可靠、无重大缺陷、可扩展、安全等），并能稳定运行。

3.1.3 服务实施检查：检查网络专线、系统迁移、部署、备份、技术支持、巡检、应急响应等服务是否按承诺实施，包括迁移方案的执行、备份策略的落实、运维记录的完整性等。

3.1.4 文档资料交付：验收是否按要求提供了完整的技术文档，包括架构图、配置资料、维护手册、巡检记录、故障处理记录、等保安全测评证书等等。

3.2. 商务履约内容

3.2.1 合同条款履行：核查双方是否严格履行了采购合同约定的各项商务条款，如付款条件、服务期限、违约责任等。

3.2.2 价格与费用：确认实际供货与服务内容与投标报价一致，无额外收费项目，所有承诺包含的费用（如迁移、升级、扩容等）均已涵盖。

3.2.3 人员配备与资质：核对中标人项目组人员是否与投标文件一致。

3.3 履约验收标准

3.3.1 依据文件：以国家及行业相关标准、招标文件、中标人投标文件、双方签订的采购合同及补充协议为主要验收依据。

3.3.2 符合性：所有交付产品及服务必须完全满足招标文件及投标文件的承诺，产品需使用国内主流品牌产品，并能通过采购人组织的功能及性能测试。如有偏离需在合理范围内经采购人与中标人双方协商并以增补协议方式进行书面确认。

3.3.3 合格条件：技术、商务各项内容均符合要求，文档齐全，采购人业务运行正常，且无遗留问题或已有明确解决方案。

3.4 履约验收其他事项

3.4.1 验收组织：由采购人组织验收小组，中标人应积极配合并提供所需条件。

3.4.2 验收程序：中标人完成项目交付或服务期满后，向采购人提出验收申请；验收时需提交满足合同约定的验收报告及相关资料（纸质版和电子版）；采购人在约定时间内依据合同中约定的验收清单进行项目验收；验收合格后双方在验收报告上进行签字确认；验收不合格的，中标人应在规定期限内整改后重新提出验收申请。

3.4.3 争议处理：验收过程中若出现分歧或验收内容及标准中未明确的事项，双方应友好协商解决。如出现变更需在合理范围内经采购人与中标人双方协商并以

增补协议方式进行书面确认。协商不成的，应当向巴彦淖尔市医院所在地人民法院提起诉讼。

3.4.4 未尽事宜：本验收内容及标准中未明确的事项，由双方在合同中详细约定，并作为验收的补充依据。

4、其他说明事项

4.1 招标人保留对招标文件的最终解释权，有权根据实际情况对招标文件进行必要的澄清、修改或补充，并将相关变更内容通知所有投标人。投标人应随时关注招标人发布的有关通知，否则由此产生的后果由投标人自行承担。

4.2 采购人对投标人在投标文件中提交的所有承诺函（包括但不限于★条款涉及的技术、服务、资质等承诺）保留全过程追责权利。自合同签订之日起至项目最终验收合格，采购人有权在任何时间对投标人承诺内容的真实性、符合性进行检查。

4.3 本项目招标文件及投标文件中所有标注“★”的条款，均为项目实施过程中的关键考核内容。中标人须在项目实施各阶段积极配合采购人进行符合性审核，按要求提供相关证明材料。

4.4 违约处理：如在审核中发现中标人存在以下情形之一的，采购人有权单方面终止合同，并要求中标人承担因此给采购人造成的直接经济损失：

- （1）提供的产品或服务与招标文件、投标文件承诺严重不符；
- （2）未按承诺履行★条款相关义务；
- （3）存在虚假应标、弄虚作假等行为。

前款所称“直接经济损失”，包括但不限于采购人重新采购所增加的费用，因系统中断导致的业务损失等可量化的损失；因项目延期导致采购人增加的其他成本（如临时替代方案费用、额外人力成本、设备租赁费用等）。