上饶市立医院
（五三院区）数据中心运维服务项目
采购文件

上饶市立医院

2025 年 10 月

目录

第一章 竞价邀请函

一、 项目概况

采购内容	数量	单位	最高限价（人民币）	采购需求	采购方式
（五三院区）数据中心运维服务	1	年	268000.00 元	详见第二章采购需求	竞价
注：1.投标人所报的报价为本项目的总报价，包括人工费、材料费、技术培训费、清运费和税金等所有费用。如有漏项，视同已包含在其它项目中，合同总价不做调整。2.投标报价高于最高限价视为无效投标。					

二、 采购文件获取及应答

获取采购文件的时间和期限、地点、方式：

有意向的供应商可从公告发布之日起三个工作日内，在江西省政府采购电子卖场（www.jxemall.com)上下载采购文件，并完成响应文件上传进行应答。

竞价截止时间、开标时间及地点：

(一) 必须在竞价截止时间前将盖章响应文件扫描件上传至江西省政府采购电子卖场，上传的电子投标文件都必须清晰，逾期或不清晰都将作无效竞价处理。

(二) 竞价截止时间和开标时间以江西省政府采购电子卖场为准。

投标有效期:自开标日起 90 个日历日。

响应文件无效的情况：

（一）资格审查过程中，出现以下情形之一的，其投标被视为无效竞价：

(1)不具备采购文件中规定的合格投标人资格要求的；

(2)未按照采购文件要求提供法定代表人身份证明书的；

(3)非法定代表人参加投标，未按采购文件要求提供法定代表人授权委托书的；

（二）符合性审查过程中，出现以下情形之一的，其投标被视为无效竞价：

(1)未按照响应文件要求的格式制作响应文件的；

(2)响应文件未按要求签署、盖章的；

(3)未按响应文件要求提供响应函、响应一览表、响应一览明细表的；

(4)响应文件未按采购文件要求编制或涂改响应文件及字迹辨认不清的；

(5)报价超过采购文件中规定的最高限价金额的；

(6)不满足采购文件中服务要求、商务要求及其他要求的；

(7)投标有效期不满足采购文件要求的；

三、 投标人资格要求

1. 具有独立承担民事责任的能力：提供营业执照副本、税务登记证副本、组织机构代码证副本（新版营业执照三证合一）复印件, 同时提供法定代表人授权委托书原件（法人参加无需提供）及法人和被授权人身份证复印件；
2. 具有良好的商业信誉和健全的财务会计制度：提供 2023 年度或 2024 年度的财务审计报告或企业财务报表，或竞价截止前 3 个月内企业基本开户银行出具的资信证明；
3. 具有履行合同所必需的设备和专业技术能力（提供承诺函）；
4. 有依法缴纳税收和社会保障资金的良好纪录： 提供竞价当月前六个月内任意一个月的缴纳证明材料（纳税发票、银行纳税转账凭证、税务局出具的纳税证明，提供任意一种均可）；提供竞价当月前六个月内任意一个月的缴纳证明材料（社保缴纳发票、交纳社保的银行转账凭证、社保局出具的正常缴纳社保证明，提供任一种均可）；
5. 参加政府采购活动前三年内，在经营活动中没有重大违法记录（提供声明函）；
6. 法律、行政法规规定的其他条件：被“信用中国”网站列入失信被执行人和重大税收违

法失信主体、被“中国政府采购网”网站列入政府采购严重违法失信行为记录名单（处罚期限尚未届满的），不得参与本项目的参询活动（提供“信用中国”、“中国政府采购网”网页截图）。

7. 本项目不接受联合体投标（提供承诺函）。

8. 本项目的特定资格要求：/

四、 联系方式

采购人名称：上饶市立医院

采购人地点：上饶市立医院

第二章 采购需求

一、 服务清单

序号	服务名称	服务模块	服务描述	交付文档	频率
1	资产管理	资产调研	纪录数据中心服务范围内各设备和系统的种类、型号、功能、物理位置、序列号、购买时间、过保时间等资产详细信息	设备清单	定期实时更新
		基础信息完善	利用设备清单进行物理设备建档，绘制网络拓扑，硬件设备物理位置图、接口对应表，完善数据中心基础信息	拓扑图	
				机柜图	
				线序表	
				业务表	
		资产信息库	利用基础信息资料建立数据中心资产信息库，将相关资料整理形成台账	台账	
		机房卫生	机房卫生清洁工作，地面卫生、设备外部除尘、储物间整理服务	/	
		线路标签	根据资产信息进行设备标签、线路标签制作粘贴服务	标签	
2	运维巡检	季度巡检	为了确保信息系统安全稳定的工作，由被动解决问题变主动发现问题，最大限度的降低系统的运行故障，周期性单位提供重要信息安全资产如安全设备、业务系统、网络设备等周期性健康检查	季度巡检报告	1 年 4 次
		年度总结报告		年度总结报告	1 年 1 次

			服务。		
3	安全服务	风险评估	风险评估通过识别资产现有的脆弱性，可能面临的威胁，并充分调研已有的安全控制措施，以综合判断存在的风险，帮助预知可能发生的安全事件，规划后期建设	风险评估报告	1 年 2 次
		基线核查	对重要服务器、应用系统、网络设备、安全设备等基于信息安全风险的角度进行配置核查，从而达到相应的安全防护要求	基线核查报告	1 年 2 次
		渗透测试	通过模拟恶意攻击者的技术和手段，来评估计算机系统、网络、应用程序或其他信息技术基础设施安全性，发现安全漏洞并修复它们，从而保障系统安全。	渗透测试报告	1 年 4 次
		安全加固	根据提供的漏扫报告和巡检报告内容进行技术加固：业务系统与信息支撑平台进行信息安全加固，包括数据安全、应用安全、操作系统、网络设备、管理制度等； 对管理层面提供建议：完善管理体系，包括人员管理、安全制度规章、系统运维等。	安全加固报告	1 年按需提供
4	应急响应	故障响应	日常信息系统故障应急响应，根据不同故障级别，提供对应的响应机制	服务报告单	1 年按需提供
		安全响应	临时性监管单位安全检查或信息系统自查进行响应，并进行检测自评估服务	监测评估报告	
		特殊事件响	针对出现安全漏洞、攻击、	应急响应	

		应	数据丢失等特殊事件进行紧急应急响应，在最短时间内妥善解决问题	报告	
			护网期间安排人员现场值守。		
5	应急演练	应急演练	提供网络及信息系统网络关键系统灾难或故障的应急演练服务，包括数据库集群切换、重要服务器切换、数据库容灾切换和云平台节点切换等。每年应急演练不少于 1 次并及时更新预案。	应急演练报告	1 年 1 次
6	网络优化	网络优化服务	基于现状，合理利旧已有设备，提供整体的改进措施和方案，提供整体网络安全保障方案，包括不限于网络的优化、策略的细化、业务的权限管控、以及一些安全制度方面的调整。	优化服务报告	1 年 2 次
7	培训服务	培训服务	基于丰富的安全运维与服务经验，提供全面深入的信息安全知识和技术与管理方面培训服务。	培训课件	1 年 1 次
			量身定制符合客户需要的信息安全技术与管理的培训，促进日常运维工作，结交行业内志同道合之人，拓展人脉圈		
8		服务器	33 台服务器		
		交换机	两机房内共 21 台交换机，内网楼层交换机共 40 台，外网楼层交换机若干，总数≥60		

	设备维保	安全设备	2 台准入、1 台数据中心防火墙	维保清单	1 年按需提供
		加密设备（吉大正元）	电子签名服务器 2 台 （原厂服务）		
		超融合服务器（EMC）	超融合服务器 4 台 （原厂服务）		
		光纤交换机	光纤交换机 4 台		
		存储务备份设备（EMC）	存储及备份设备共 4 套 （原厂服务）		
		UPS	两机房共 3 套 UPS 主机（不含电池）		
		精密空调	精密空调 2 套		
10	重保值守要求	重保值守	在国家重大节日或者重大活动期间提供安全保障服务，包括但不限于护网活动（省、市级）、两会、重大节假日等重要时期的现场保障，按医院需求提供安全保障，包括事前隐患排查、重要系统巡查、安全加固、安全值守、设备借用、事件处置、原因分析、事后总结等。		1 年按需提供
11	运维服务平台	运维服务平台	对应用软件、数据系统、虚拟化系统、硬件系统提供 7×24 自动化监控服务，包括性能监控和可用性监控。 虚拟化系统：vmware 虚拟		1 年按需提供

			化相关资源 数据系统：数据库、中间件、应用系统； 硬件系统：服务器（含操作系统：国产操作系统、linux、windows server等）、网络（交换机、路由器、防火墙、IPS 等网络和安全设备）、存储等物理资源；		

二、 服务要求

（1）信息资产统计及管理服务

此项服务详细调查并记录服务范围内的各个设备的种类、型号、功能、物理位置、端口对应情况、部署情况等资产信息，然后录入管理系统。在服务有效期内，持续关注数据中心内的资产变更情况，并及时录入系统，只需轻点鼠标即可纵览整个数据中心的资产使用情况。

在管理硬件资产的同时，能同时对 IP 地址、虚拟化资源、配置文件等进行管理。通过图形化的界面，能准确知道 IP、应用、服务器（物理或虚拟）、机柜、网络接口、业务负责人之间的一一对应关系。

在 IP 地址管理上，同时提供 IPV4 及 IPV6 地址空间的管理，能准确的了解网络内 IP 地址的使用及分配情况。

（2）网络配置文件管理

此项服务主要提供网络设备的自动配置文件管理功能，减少人工文件管理带来的复杂性，提供配置合规性管理、批量配置部署等功能。

在服务有效期内，对数据中心内的设备配置进行自动定时备份，在设备因为意外原因导致配置文件丢失时，及时恢复到指定时间点的配置。

（3）硬件运维基本服务：

负责对运维设备所有硬件做故障诊断及系统性能维护。有充足的备机备件，保障核心设备出现故障后，可无偿提供备用设备服务，对所有运维设备的故障件均给予技术支持，提供维修服务，维修前须能提供备品备件的能力。提供对扩容设备进行安装调试。确保发生故障的情况下能迅速提供备机并且备机系统能够正常接管生产机的工作，保证业务不停止。

备品备件要求：

a.有充足的备品备件；

b.设备故障无法在短时间内修复时，投标人必须 12 小时内提供备件到现场；

（4）系统软件维护基本内容

提供对工具类系统,包括备份系统、虚拟化系统、日志系统及所有 ORACLE 版本升级（或安装新版本）、故障维护及性能优化调整，如果不能在 4 小时之内解决系统软件问题，采购方将有权请第三方技术人员上门维护，费用由中标方承担。

1)故障响应及处理：

a.对系统性能严重损坏，接到支持需求必须立即做出回应；

b.对系统运行正常，仅受到有限的影响或未受到严重影响，接到支持需求必须在 30 分钟内做出回应；

2)服务工程师：技术维保工程师应具备上述维保对象的硬件系统、软件系统、管理及操作系统等方面的知识，具备相应的技术资格认证，并有 3 年以上从业经验；

3)产品升级：提供产品升级评估和升级服务。

（5）数据库系统维护基本内容

提供 ORACLE 数据库系统 7X24 小时电话技术支持服务。当遇到紧急事故，或者系统迁移、安装等重大问题，通过前期电话沟通后，在最短的时间内派出具有 ORACLE 认证的现场技术支持工程师（OCP 认证级别及以上）在 30 分钟响应，当远程无法解决时 4 小时内到达现场，提供现场技术服务。

1）系统安装、优化服务

提供 ORACLE 数据库软件的安装、配置服务，在系统环境满足 ORACLE 安装需求的前提下，保证数据库系统能够正确安装、配置，直至能够交付正常使用。

根据需要，指定的 ORACLE 数据库服务平台，进行系统级和数据库级的调优工作：专业技术工程师根据系统环境(硬件配置、操作系统、数据库系统)，以及多年的系统和 ORACLE 的实践经验进行调优工作。

2）系统检查服务

每季度指定具有 ORACLE 认证的专业技术工程师到现场进行对 ORACLE 数据库系统进行检查(例如：ORACLE 表空间使用状态、ORACLE 警告日志、数据备份执行情况…等等)。同时巡检工程师负责向客户提供现场咨询服务，咨询范畴包括硬件配置、应用软件性能分析/合理化建议等。

3）ORACLE 数据库升级服务

在厂商必要的补丁或升级产品推出后，提供升级资讯。在接到 ORACLE 数据库升级需求后，派出具有 ORACLE 认证的现场技术支持工程师将的 ORACLE 数据库软件升级至最佳版本。

4）数据迁移服务

根据的数据迁移需求，派出具有 ORACLE 认证的现场技术支持工程师，将原系统的数据移植到新系统上的 ORACLE 数据库之中，并保证数据的完整性和可用性。

5）数据库备份与恢复服务

在数据库系统第一次安装完毕时，在现场制定备份策略、搭建数据备份系统；在数据库系统遇到重大问题时，在 30 分钟响应，当远程无法解决时 4 小时内到达现场，进行系统恢复；

6）数据库故障应急服务

当的数据库系统出现各种意外情况(如系统崩溃、硬件损坏、电源掉电等)造成数据库不能正常使用情况，在接到故障电话后在 30 分钟响应，当远程无法解决时 4 小时内派出具有 ORACLE 认证的专业技术工程师将到达现场，进行故障的分析、排查，并最终保证其恢复可用(在严格按照既定的备份策略执行的前提下，保证数据不丢失)。

（6）定期现场巡检服务

每季度对数据中心进行全面检查的服务项目，通过该服务可使客户获得设备运行的第一手资料，最大可能地发现存在的隐患，保障设备稳定运行。同时，有针对性地提出预警及解决建议，能够提早预防，最大限度降低运营风险。

巡检包括但不限以下内容：

机房环境内容巡检，定期对机房的温湿度监控设备、UPS 监控设备、消防监控设备等机房环境监控设备的温湿度、电压、电流、烟雾等关键工作指标进行例行监控，当发生异常情况时，及时进行跟踪和处理。

机房设备硬件情况巡检，机房网络情况巡检,对整个网络健康状态进行分析，定期对各网络安全设备的 CPU 利用率、内存利用率、磁盘利用率、端口流量、报警信息等关键工作指标进行例行监控，当发生异常情况时，及时进行跟踪和处理；网络及安全设备配置管理、网络系统流量分析、网络及安全设备日志分析、软件升级。

机房主机安全巡检，利用现有的漏洞扫描设备全网扫描、分析上述系统的安全漏洞，及时发现安全隐患, 备份系统日常维护，状态检查，故障处理等。

服务器操作系统、应用系统、数据库安全巡检，存储及磁带库数据安全巡检。

机房信息变动情况收集整理、文档更新。

（7) 信息安全服务

1）根据江西省和上饶市信息安全工作相关要求对上饶市立医院管辖的包括业务系统、服务器、网络设备、安全设备等所有信息系统资产在内的信息系统进行信息安全风险评估；

2）对医院的信息系统进行全面梳理，协助医院依据信息系统的现状完成等级保护相关工作。

3）.定期提供业务系统服务器漏洞扫描、对外服务网站应用层漏洞扫描、网页防篡改状态检查、互联网安全保护技术状态检查、业务系统服务器恶意代码防范工具状态检查、个人终端漏洞扫描测试，并协助上饶市立医院对发现的问题和漏洞进行修复。

4）.对医院提供安全防范技术措施落实情况核查与优化、应急预案建设与演练、公众服务系统安全检测、安全培训等安全服务。

5）.完成上级主管部门信息安全检查所需要的相关工作。

项目内容明细及要求

安全目标

根据医院信息系统网络、应用及数据等方面安全需求，针对保护目标及结合等级保护基本要求，通过安全评估、安全巡检、协助加固、应急响应等服务，针对服务实施前与实施后防护效果进行打分，能够直观地、具体量化地展现安全服务效果和服务价值，有效降低网络安全和数据库安全风险。

安全服务内容

7.1 信息系统安全风险评估

通过人工安全评估服务从多角度审查，全面模拟黑客的方式评估信息系统的安全状况，识别安全威胁与脆弱性，分析与监管要求的差距，出具分析报告和改善方案。评估范围包括组织范围，比如某些部门；物理范围，比如机房、办公区域等；系统范围，比如主机、数据库、中间件、网络设备、安全设备、重要信息系统、相关管理制度等。安全评估内容应包含网络架构安全评估、主机系统安全评估、数据安全评估、应用安全评估及整体安全策略评估五大块内容。

具体要求包括：

网络架构安全评估：包括结构安全与网段划分评估、网络访问控制评估、接入访问控制评估、网络安全审计评估、边界完整性检查评估、网络入侵防范评估、恶意代码防范评估、网络设备自身防护评估。

主机系统安全评估：包括身份鉴别、自主访问控制、安全审计、系统保护、剩余信息保护、恶意代码防范、资源控制等方面评估。

数据安全评估：包括数据保护评估、数据完整性评估、数据保密性评估、安全备份评估。

应用安全评估：包括身份鉴别、访问控制、安全审计、剩余信息保护、通信完整性、通信保密性、软件容错、资源控制、代码安全等方面。

整体安全策略评估：依据物理安全、网络安全、主机安全、应用安全、数据安全等五个方面评估结果，同时考虑在信息安全管理体系等其他互补因素,然后进行全面的安全策略有效性评估。评估结果作为后期加固依据。

7.2 漏洞扫描服务

采用扫描工具结合人工验证对本项目的信息系统进行脆弱性评估，获得应用、数据库、系统、设备等漏洞对应及分布情况，并提供可操作的安全建议，并进行安全加固。

漏洞扫描所采用的工具须满足以下条件：

具有计算机软件著作权登记证书；

具有兼容性资质证书；

软件产品登记证书；

涉密资质产品检测证书；

7.3 安全检查服务

人工结合工具对服务范围的网络设备、主机设备、操作系统、数据库、应用中间件等进行设备安全配置、主机配置、数据库配置、应用配置等方面的安全基线检查。根据检查结果提出整改建议，协助运维管理人员开展整改工作。

7.4 7*24 小时日志分析服务

定期对内网全网日志中的高级别日志进行分析，对安全事件进行溯源、满足《网络安全法》日志存储不少于 6 个月的要求，并出具分析报告。结合人工方式，利用综合日志审计平台、设备、系统自身的日志数据进行综合分析，判断网络、操作系统、应用中间件、网络安全设备等资产的整体运行情况、安全状况等，直观展现上述内容给，提出整改意见，帮助整改。

7.5 协助安全加固服务

根据各类安全评估结果的具体情况，制定服务目标的整改加固建议。针对不同类型的目标系统，协助进行安全加固处理，合理加强服务目标的安全性。完成整改后开展复查工作。

7.6 应急预案与应急演练

依据实际情况为作为医院信息系统建立网络安全应急预案，组织网络安全事件应急相关人员在有计划及受控制的情况下，依据预先制定的网络安全应急预案执行可预见的减少信息系统停顿、失败或灾难影响的预案措施。使相关人员熟悉应急响应、处置过程，尽可能消除信息系统所出现的中断，保护系统免受重大故障或灾难的影响，缩短系统中断的恢复时间。

7.7 应急响应服务

网络没有绝对的安全，在确保安全设备合理部署及安全服务保障情况下，具备 365*24 小时的应急响应服务。如单位网络管理员或系统管理员根据初步判断认为和安全事件相关，通过电话咨询服务商安全专家，安全专家再根据安全事件级别进行应急响应，其目的是最快速恢复系统的保密性、完整性和

可用性，阻止和降低安全威胁事件带来的严重性影响。安全事件包括但不限于：病毒和蠕虫事件、黑客入侵事件、内容篡改事件、信息泄漏事件等。

7.8 安全培训服务

为协助医院提高内部人员的安全意识、安全技术能力及安全管理能力等，针对管理和技术两个层面制定阶梯性人员能力培训计划，通过安全培训使相关人员的安全能力有明显提升。培训讲师需具有至少一项信息安全专业资质，如 CISSP、CISP、ISO 27001 LA、等级保护测评师认证资质。

培训内容：《网络安全基础培训》、《数据库运维基础培训》

7.9 新系统上线测试

提供新业务系统上线安全测评服务，识别新系统主机、中间件、数据库、应用等潜在安全风险，针对发现的安全隐患制定有效处置方案，降低新业务系统风险系数，建立一体化新业务安全检测体系，检测数据成果作为新上线安全建设参考依据。

新系统上线安全检测具体要求：

对新业务系统系统进行主机漏洞扫描，以发现目标新业务系统系统的全弱点为目标。

对新业务系统中指定网页范围进行新业务系统高危脚本漏洞挖掘验证，包括 SQL 注入、XSS 攻击、恶意执行逻辑错误等典型脚本漏洞信息。

对新业务系统进行网络安全脆弱性检测。

对新业务系统进行渗透测试。

7.10 重要时刻值守服务

在重大节假日、重大活动期间，提前进行信息系统安全专项检测，并提交检测报告。当认为必要时，重大割接或其它任何客户认为可能对其业务运营产生重大影响的时刻，提供 7*24 小时的现场值守服务。

7.11 安全服务的要求

1、提供 7*24 小时的技术支持（包括电话咨询与现场服务）。

2、在接到电话后，必须在 30 分钟内响应，当远程无法解决时 4 小时内必须到达上饶市立医院现场。

3、每次对系统进行安全评估、安全扫描、渗透测试、安全加固之前必须要先提供相应的技术方案与业主方技术人员充分沟通，以确保系统的安全运行。

4、实施过程中应尽可能小的影响系统和网络的正常运行，做好备份和应急措施，不能对医院系统内的应用系统的正常运行产生影响，包括系统性能明显下降、网络拥塞、服务中断等，如无法避免出现这些情况应先停止项目实施，并向业主方书面详细描述。

5、所使用的信息安全类工具软件（包括 web 应用安全评估系统、数据库安全评估软件系统、远程安全检查工具、大数据分析平台等）必须为正版产品，并进行详细说明。

6、项目服务过程的数据和结果数据严格保密，未经业主方授权，任何机构和个人不得泄露给其它单位和个人。

7、协助业主方完成各项年度安全检查工作。

8、服务提供商必须签订保密协议，做好相关信息数据保密工作，承担保密责任。不得对外透露与相关的设备、网络和系统信息，不得复制与相关的数据和信息，不得以任何方式和渠道向外界传递、泄露、披露任何信息数据。

（8）虚拟化运维服务

此项服务主要涵盖故障排除、日常巡检、性能检查及优化、数据安全保护、产品培训等多个方面。

日常巡检及检查优化方面，结合历史数据及原厂商工具，预测分析虚拟化平台未来的业务增长情况，及时发现潜在问题，避免资源过度使用及不足等情况的发生。

数据安全保护主要提供虚拟化平台的集中备份与恢复方案、协助进行数据迁移及应急预案的制定。

网络安全上帮助解决虚拟化平台上虚拟机之间流量互通带来的安全威胁，进行端口隔离，实施基于主机的虚拟防火墙，对访问流量进行控制。

（9）备品备件服务

提供备品备件服务，服务器、存储、交换机、安全设备等核心硬件产品备件，当设备故障可提供备品备件以保障应用稳定运行。对所有运维设备的故障件均给予技术支持，维修前须提供备品备件。在发生故障的情况下能迅速提供备机并且备机系统能够正常接管生产机的工作，保证业务不停止。

（10）容灾演练

服务期内不少于一次核心系统灾难备份及恢复的应急演练。

三、 商务要求

1．服务期限：一年。

2．服务地点：上饶市立医院。

3．付款方式：合同签订后 20 个工作日支付合同金额的 80%，服务期满后 10 个工作日内支付合同金额的 20%。

4. 售后服务：

（1）自合同签订之日起，为上饶市立医院（五三院区）数据中心提供一年的运维服务。

（2）服务期内，应当提供 7×24 小时响应支持服务，对于紧急故障（如导致业务中断的故障），运维团队响应时间不超过 30 分钟，故障修复平均时间不超过 4 小时；对于非紧急故障，响应时间不超过 60 分钟，故障修复平均时间不超过 8 小时。设备故障无法在短时间内修复时，投标人必须 12 小时内提供备件到现场供采购人使用，直至故障产品修复。

（7）针对本次项目提供详细的售后服务方案。

四、 其他要求

1、 供应商所提供的运维服务平台需满足以下要求：

（1）具有云端管理功能。用户部署的运维服务平台可接入云端平台。用户登录云端平台，可以实时查看每个监控系统的监控整体状况、实时故障通知信息。用户系统通过云端系统实时推送微信告警通知。（提供平台截图加盖投标人公章）。

（2）通过云端平台，在微信服务号上，可浏览网管和动环的整体健康度、监控统计信息。浏览网管分类分组统计，监控设备健康度、告警详情、监控内容可用性分析柱状图、指标性能曲线图。浏览动环分类分组统计，动环监控内容和指标。（提供平台截图加盖投标人公章）。

（3）服务器操作系统监控 Windows 需同时支持 SNMP、客户端等多种方式进行监控。客户端支持对 Windows 硬件状态、资产信息（CPU、内存、主板、显卡、磁盘、raid 卡、电源、电池、风扇等）的全方位的采集监控（提供平台截图加盖投标人公章）。

2、 中标人必须于中标后 5 个工作日内，提供运维服务平台功能演示，未提供者视为虚假响应，将取消其中标资格。

参与竞价的供应商需充分了解本项目的需求，按要求提供相应的响应材料，上传响应文件并加盖公章，对于虚假应标的行为保留对该供应商追究相关责任的权利。

第三章 响应文件格式

响应文件

项目名称：

项目编号：

投标人：（章）

法定代表人：（签字或盖章）

投递日期：

一、 响应函

致：上饶市立医院

根据贵方为（项目名称）采购需求响应文件的要求，提交下述响应文件一份：

1.响应函

2.响应一览表

3.响应一览明细表

4.服务要求响应、偏离说明表

5.商务要求响应、偏离说明表

6. 法定代表人授权委托书

7. 法定代表人身份证明书

8.响应人资格声明函

9.资格证明文件

10. 技术文件

据此函，我单位宣布同意如下：

1.所附投标价格表中规定的应提交和交付的项目投标价为大写：整 (小写：元）（用文字和数字表示的投标总价）。

2.本投标有效期为自开标日起（）个日历日。

3.将按采购文件的规定履行合同责任和义务。

4.已详细审解读全部采购文件内容。

5.同意提供按照贵方可能要求的与其采购有关的一切数据或资料。

6.承诺：不得将本次采购或合同的有关资料向第三方透露。

投标人：（盖章）

法定代表人或授权代理人：（盖章或签字）

日期：年月日

二、 响应一览表

序号	项目名称	总报价	服务期	服务地点	备注
		人民币：整（￥：元)			

投标人：（盖章)

法定代表人或授权代理人：（盖章或签字)

日期：年月日

三、 响应一览明细表

序号	服务名称	单价(元)	总价(元)	备注
	合计：人民币：整（￥：元)			

投标人：（盖章)

法定代表人或授权代理人：（盖章或签字)

日期：年月日

四、 服务要求响应、偏离说明表

序号	招标项目要求	投标人响应	响应或偏离	说明

注:

1)“招标项目要求”：按采购文件对“第二章采购需求中的服务清单和服务要求”逐一列明。

2)“投标人响应”：对“招标项目要求”逐一具体响应内容，未列明视为负偏离。

3) “响应或偏离”：注明对招标项目要求响应或偏离情况。

4) “说明”：对偏离情况进行说明。

投标人：（盖章）

法定代表人或授权代理人：（盖章或签字）

日期：年月日

五、 商务要求响应、偏离说明表

序号	招标项目要求	投标人响应	响应或偏离	说明

注:

1) “招标项目要求”：按采购文件对“第二章采购需求中的商务要求”逐一列明。

2) “投标人响应”：对“招标项目要求”逐一具体响应内容，未列明视为负偏离。

3) “响应或偏离”：注明对招标项目要求响应或偏离情况。

4) “说明”：对偏离情况进行说明。

投标人：（盖章）

法定代表人或授权代理人：（盖章或签字）

日期：年月日

六、 法定代表人授权委托书

本授权委托书表明：本人（姓名）系（投标人名称）的法定代表人，现授权委托（姓名）为我公司代理人，以本公司的名义参加（招标单位）的项目的投标活动。代理人在开标、评标、合同谈判过程中所签署的一切文件和处理与之有关的一切事务，我均予承认。

代理人：性别：年龄：身份证号：

单位：部门：职务：

代理人无转委托权。特此委托。

注：后附代理人身份证扫描或复印件。

投标人（盖章）

法定代表人（盖章或签字）

日期：年月日

七、 法定代表人身份证明书

（上饶市立医院）：

_____同志，（身份证号码：）在我单位任职务，是我单位的法定代表人。

特此证明

身份证(或其它有效身份证明)复印件粘贴处

投标人名称（盖章）：

法定代表人（签字或盖章）：

年月　　日

注：法定代表人本人参与投标的，须提供此表，无须提供《法定代表人授权委托书》。

八、 响应人资格声明函

致：上饶市立医院

我公司自愿参加（项目名称）项目（项目编号：项目编号）的投标。我公司对此次投标项目作如下声明：

1、投标文件中提供的所有关于投标人资格的文件、证明、材料、陈述均是真实的、准确的。

2、我公司近三年没有因腐败或欺诈行为而被政府或业主宣布取消响应资格或在经营活动中没有重大违法记录。

若有弄虚作假，我公司愿意按照采购文件要求及相关规定接受处罚，包括取消中标资格、没收投标保证金，并承担由此产生的一切后果。

特此声明！

投标人名称（公章）：

公司地址：

法定代表人（签名或签章）：

联系电话：

投标日期：　　年　月　日

九、 资格证明文件

1. 具有独立承担民事责任的能力；

2. 具有良好的商业信誉和健全的财务会计制度；

3. 具有履行合同所必需的设备和专业技术能力；

4. 有依法缴纳税收和社会保障资金的良好纪录；

5. 参加政府采购活动前三年内，在经营活动中没有重大违法记录；

6. 法律、行政法规规定的其他条件。

7. 本项目不接受联合体投标（提供承诺函）。

8. 本项目的特定资格要求：/

十、 技术文件

采购文件要求提供的其他材料