采购需求

说明：“★”号标注的内容为实质性要求，必须满足或优于该要求，否则按照**无效投标**处理。

一、项目概况

（1）项目名称：2026 年武汉市东西湖区交易中心数据存储服务

（2）采购单位：武汉市东西湖区行政审批局

（3）项目概况： 为保障建设工程及政府采购项目相关信息的保密性，确保平台项目开评标过程稳定进行，同时加强系统安全防护，减少被攻击风险，保证数据安全可靠，按照全局网络安全相关要求，交易中心现有的不见面开标系统及政府采购电子交易系统相关数据及服务器均需部署至云服务器，以满足安全管理要求。结合上述两系统运营方提出的云资源配置方案，现需采购对应的存储服务（含云主机、云硬盘、网络通信及安全防护等服务）以支持系统运行。

不见面开标系统的存储服务主要包含：智慧化系统、实时的开评标过程和历史存档的音视频监控、项目电子档案和云上加云下存储共用。

政府采购电子交易系统的存储服务主要包含:项目前期的招标与采购文件、中期的投标响应文件，以及后期的开评标过程资料等关键业务文档。

（4）项目地点：武汉市东西湖区公共资源交易中心。

二、采购内容

包号	标的序号	品目名称	品目分类编码	计量单位	数量	预算金额（万元）	是否进口
1	1	2026 年武汉市东西湖区交易中心数据存储服务	C16030100 存储服务	项	1	52	否

云存储服务明细表

一、云资源服务				
1.云主机				
序号	服务项目	服务说明	计费单位	数量
1	云主机	2 核 vCPU、8GB 内存、40G 系统盘	台/年	2
2	云主机	8 核 vCPU、16GB 内存、40G 系统盘	台/年	8
2.云存储				
序号	服务项目	服务说明	计费单位	数量
1	云硬盘	每 1GB 高速云硬盘	GB/年	34,200
3.网络通信				
序号	服务项目	服务说明	计费单位	数量
1	电子政务外网带宽	100Mbps 单线电子政务外网带宽含 2 个政务外网 IP	1Mb/年	100
2	互联网带宽	独享单线互`联网带宽（最小开通带宽为 1Mb，计数单位为 1Mb）	1Mb/年	200
3	公网 IP 地址	公网 IP 地址（最小订购为 1 个，计数单位为 1 个）	每个/年	2
4.云安全服务				
序号	服务项目	服务说明	计费单位	数量
1	堡垒机	针对云上运维安全的管控，本服务提供： 1、运维账号集中管控服务，实现对所有被运维的 IT 资产账号的集中管理和监控；2、运维身份强制认证，支持双因素认证，对运维人员提供统一的访问入口及强制的身份验证机制；3、统一资源授权，提供运维人与设备对应关系，最大限度保护用户资源的安全；4、集中访问控制，	5 个 IP/年	2

		支持命令集细粒度的权限控制，减少误操作导致系统受到破坏；5、集中操作审计，对运维人员操作集中审计，出现问题能快速定位并进行准确溯源；6、会话场景全程回放，提供视频回放的审计界面，以真实、直观、可视的方式重现操作过程；按管控的 IP 数量计费，每 5 个 IP 管控对象为 1 个计费单位，采用包年计费。		
2	入侵防御服务	通过建立主机和服务器的行为数据模型进行异常行为检测，支持对底层的 ARP 攻击、网络攻击、20 多种常见协议的异常、病毒蠕虫木马、恶意 URL 等一系列入侵威胁进行检测及防御。按接入 IP 数量采用包年计费。	每 IP/年	2
3	网络防火墙	提供云平台基础防火墙，对云平台东西向、南北向网络进行防护。	每 IP/年	1
4	VPN 接入	10Mbps 专用 VPN 接入互联网带宽	条/年	1
5	漏洞扫描服务	全方位检测系统存在的脆弱性，包括：操作系统、数据库、中间件、Web 应用等，发现系统存在的安全漏洞，检查系统存在的弱口令，收集系统不必要开放的账号、服务、端口，对系统中多个方面的安全脆弱性统一进行分析和风险评估，形成整体安全风险报告。按 IP 数量计费，每 5 个 IP 对象为 1 个计费单位，采用包年计费，每月提供一份安全评估报告（电子版）。	5 个 IP/年	2
6	日志审计	日志审计服务内容包括： 1、将安全系统、主机操作系统、数据库等系统的日志、事件、告警汇集起来，实现对安全信息（日志）进行统一监控。 2、基于安全监测、告警和响应技术的事件关联分析引擎。在关联规则的驱动下，事件关联分析引擎能够进行多种方式的事件关联。 3、对日志进行全面分析与审计，集成各种合规性关键控制点需求，为用户提供合规性审计报表报告	每主机/年	10

7	云主机防病毒服务	结合云查杀引擎、脚本查杀引擎、启发式查杀引擎、人工智能查杀引擎、系统修复引擎、主动防御技术，有效查杀已知和未知病毒	每主机/年	10
8	云主机系统安全防护	包含以下功能： 1、防病毒，通过云主机安全代理软件，有效查杀主机上的文件、内存、进程中的恶意程序； 2、WebShell 防护，包含了 40 万以上的网站后门样本和大量的后门特征码，双重机制保证对于样本的有效检测与查杀； 3、防暴力破解，可以有效防御远程桌面和 SSH 登录的暴力破解，保障主机的安全； 4、主机入侵防御，可实现主机的入侵防御功能，包括防御新型漏洞、病毒攻击，阻拦可疑的行为等； 5、网卡流量统计，可查看各个云主机网卡的流量情况，实现各主机流量的统一管理查看。	每主机/年	10
9	Web 应用防火墙	对 Web 的业务流量进行恶意特征识别及防护，提供 Web 服务器漏洞防护、Web 插件漏洞防护、爬虫防护、跨站脚本防护、SQL 注入防护、LDAP 注入防护、SSI 指令防护、XPATH 注入防护、命令行注入防护、路径穿越防护、远程文件包含防护等服务，将正常、安全的流量回源到服务器,避免网站服务器被恶意入侵，保障业务的核心数据安全。按实例数量采用包年计费。	每实例/年	2
10	网页篡改在线防护	实时过滤 HTTP 请求中混杂的网页篡改攻击流量（如 SQL 注入、XSS 等），监控网站所有需保护页面的完整性，采用文件级驱动保护技术，用户每次访问每个受保护网页时，Web 服务器在发送之前都进行完整性检查，保证网页的真实性，当检测到网页被篡改时，第一时间发出告警信息，对外仍显示篡改前的正常页面。按实例数量采用包年计费。	每实例/年	1

11	域名证书ssl	网站安装 SSL 证书后，使用 https 加密协议访问网站，可激活客户端浏览器到网站服务器之间的"SSL 加密通道"(SSL 协议)，实现高强度双向加密传输，防止传输数据被泄露或篡改。	个/年	1

三、技术要求

1 云服务平台要求

1.1云服务平台专用要求

★云服务平台的云服务器、云存储、系统软件、网络等资源为政府各级政务部门及具有行政审批职能的事业单位专用。（提供加盖投标人公章的承诺函，格式自拟）

1.2云服务平台性能指标

单集群支持的最大虚拟机数量不少于1000；

单个虚拟机支持的vCPU数量不少于32；

单个虚拟机支持的网卡数量不少于4；

单个虚拟机虚拟磁盘数量不少于4；

单个虚拟机支持的内存容量不少于128G；

单个虚拟机最大虚拟磁盘容量不少于16TB；

虚拟机支持主流的windows和linux客户操作系统。

1.3云服务平台网络互联要求

云平台应具备接入电信、移动、联通、等主流国内运营商网络的能力。供应商应具备接入武汉市电子政务网络的能力。

1.4云服务平台技术要求

为便于维护，构建云平台的底层操作系统应为开放的操作系统，不得使用定制化操作系统；

云平台所使用虚拟化技术为开放的虚拟化技术，如：KVM、XenServer、VMware vSphere；

云平台具备功能完整、架构完善、体系完备的服务能力，如云服务器、负载均衡、云存储、云安全、网络等服务产品；

服务商除服务目录中所列标准产品，可为用户提供定制化的云服务产品；

云平台支持部署主流数据库，包括并不限于 Oracle、MySql 及国产数据库；支持对不同资源对象进行监控。

支持基于SNMP、IPMI等多种不同监控协议，实现IT基础设施的统一管理。

支持丰富多样的监控指标，包含CPU、内存、存储、网络等。展示集群中物理机、虚拟机的数量，物理机、虚拟机的CPU平均使用率、内存平均使用率、磁盘I/O平均速率、网络I/O平均速率等，展现资源使用TOP排行情况。

支持以大屏监控拓扑分布的方式，展示当前云平台资源的规模、分布及状态信息，全屏展示数据中心的总体概要信息。

支持虚拟机使用效率统计。支持对一段时间内，虚拟机资源使用效率的统计，包含CPU使用效率统计，内存使用效率统计，存储使用效率统计等。相关报表可通过邮件定时发给指定人员。

支持任务管理，可在任务管理界面直观的展示虚拟机任务进度情况。

支持基于虚拟机的监控报表。可以生成虚拟机CPU、内存、磁盘、网络、运行时长的报表，并可以以天、周、月、年为单位或自定义时间范围生成统计及趋势报表。

通过对性能指标设置精确的告警条件定义组合，准确告警系统运维状况，并能触发电子邮件通知管理员，提高系统运维效率。

1.5云平台运营管理要求：

提供用户及资产的全生命周期管理，支持用户、用户组的创建、修改、删除；支持虚拟机创建、启动、关闭、重启、修改、分配、回收、销毁等操作。

支持生成虚拟机随机密码，在创建或申请时允许用户进行自定义的配置。

提供资源申请审批流程和资源分配流程两种资源分配模式。用户可根据需要申请对应资源，最终由管理员审批后获得资产，也可以由管理员直接给用户分配资源而获得资产。

支持多租户管理，用户层级不少于3级。支持不同用户角色，不同的角色具有不同的访问权限。

支持用户组，管理员可以对组织进行创建、修改、删除等操作，为组织分配CPU、内存、硬盘、网络等资源。

支持在组织内部进一步划分子组织，将组织内人员和资产放入项目组中，使项目组成员可对项目组中的物理主机、虚拟机等资源进行共享和使用。

支持将数据中心物理资源整合成VDC（虚拟数据中心）。管理员可根据需要对数据中心的物理资源进行划分，满足不同业务对物理资源的差异化需求。

采用丰富多样的资源隔离技术，包括基于用户访问权限控制和虚拟网络隔离技术等，使每个租户拥有独立的云资源，实现多租户环境下的安全性和可靠性。

2 云主机服务要求

云主机业务为用户提供申请即用的虚拟机业务，用户可以根据业务需要灵活申请指定CPU/内存/磁盘/网卡规格、指定OS类型的云主机用于满足各类应用的计算需求。

应提供云主机模板，可按用户要求创建不同规格的云主机，自定义 CPU、内存、网络、磁盘等属性。

支持对不同用户的云主机CPU、内存以及VPC和安全组防火墙的网络级别的隔离，确保不同用户之间数据互不可见。

支持云主机的动态升级、快照备份、性能监测分析、异常告警、日志管理等功能。

支持云主机自定义快照能力，支持对运行或停止状态的虚拟云主机生成快照，应提供分钟级别快照回滚功能；

支持云主机资源快速地动态伸缩；

支持多种资源自动调度策略，满足不同业务系统的SLA需求；

应具有人工迁移云主机功能，以便维护人员维护服务器时将云主机迁移到其他服务器的云主机；

应支持云主机容灾功能，支持主机复制方式、阵列复制方式和存储双活容灾方式。

应支持多种操作系统，包括并不限于主流的Windows、Linux等；

应支持云主机计算、网络和存储QoS能力，满足云主机的服务质量要求；

应支持管理较大规模服务器集群的能力。

3 云存储服务要求

云存储为云主机提供的低时延、持久性、高可靠的数据存储服务。

云存储应基于业界成熟稳定的存储产品搭建，可提供弹性扩展的存储资源。应具有更高的数据可靠性，更高的I/O吞吐能力，更加简单易用等特点，可适用于文件系统、数据库等系统软件或应用。

可提供实时监控云硬盘读写速率、读写操作速率、读写流量以及IO监控的信息，了解云存储运行状况。

4 网络资源要求

供应商应为本项目接入武汉市电子政务网络，并为本次项目提供 100Mbps 武汉市电子政务外网带宽和 100Mbps 电子政务专网带宽，并可根据采购人要求增加或降低政务网络带宽。

5 云安全服务要求

云安全参考传统信息安全防护手段，并增加基于虚拟化技术的防护要求，满足面向云的全面安全防护，主要包括通信和网络安全、虚拟化安全、运行安全、信息安全和管理安全。

投标人为本项目提供服务的云平台系统需获得信息系统安全等级（不包含采购人信息系统等级保护测评及其费用）第3级或以上级别备案证明。

云平台须为本项目提供以下安全服务进行保障：

基础防火墙防护服务

5.1通信和网络安全

当不同业务使用云网络传输时，应分别符合采购人对各个网络的安全管理规定或标准；

专网专用，当网络之间需要进行数据交换时，应采取相应措施保障网络安全；

当不能解决云范围内多网的隔离问题时，宜设置多套完全物理隔离的监控系统，分别直接连接相应网络进行监控。

防火墙策略按照最小开通原则，仅开通客户需要的端口。

对虚拟机模板定期进行安全加固，裁剪应用程序不必要的功能和服务，减小虚拟主机的潜在攻击面，防止被恶意篡改；

5.2运行安全

实时监测网络数据流，监视和记录内、外部用户出入网络的相关操作，使用防火墙等工具提高网络通信的安全性；

应制定安全应急处理预案，对于在正常工作中发生的突发事件，应由值班人员或维护人员依照应急处理预案进行处置或自动降级处理；

建立完善的安全管理制度，对数据中心的工作人员应进行安全管理教育和定期培训，应对云的各种设备、组件、服务进行定期安全检查和维护。

5.3运维管理安全

云平台服务严格遵从国家和行业的各项法律法规和规章制度、政策、服务指南、标准与协议，遵从法律和法规要求的最高水平，为用户提供高度安全、符合政策要求的云服务。

云平台将对用户隐私、数据的保护放入云服务合同中，严格执行。所有参与云平台运维的技术人员，均需签署《保密协议》。

云平台尽量避免和减少个人数据的使用，尽可能依照法律要求使用匿名或化名。采取适当的技术措施和组织措施来保护用户的个人数据，以防止对数据任何非法形式的处理。这些措施应当确保一种与数据处理表现出的风险以及被保护的数据的性质相适应的安全水平。

云平台禁止并非最终用户的其他人在没有得到相关最终用户同意的情况下，通过收听、偷听、存储或其他的形式来拦截或监视其通信及相关的数据流。

云平台云服务建设可靠、安全及具有恢复能力的网络，保障网络稳定安全运行；任何组织或者个人不得危害客户网络或利用网络从事危害任何国家安全、社会公共利益或者他人合法权益的活动。

云平台应实行7*24小时，全年无间断运维监控，实时发现云平台环境及用户环境出现的各种问题，及时解决。

应由专业的运维工程师，每天至少两次，对云平台的硬件设备进行现场检查，及时发现硬件设备问题，随时处理。

云平台整合专业的运维监控平台软件，对云平台环境进行全天候自动监控，实施发现问题，及时处理。

6 服务项目指标要求（日常响应和重大保障响应）

服务项目	类别	方式	指标	备注
虚拟服务器云平台资源及服务运行时间			7×24 小时	
定期监控频率			5 分钟	
云平台资源可用性			99.95%/月	
紧急、严重情况响应时间	工作时段	电话	<15 分钟	遇忙线<30 分钟

		邮件	<30 分钟	紧急邮件
	非工作时段	电话	<60 分钟	
		邮件	<4 小时	
非紧急、严重情况响应时间	工作时段	电话	<2 小时	
		邮件	<4 小时	
	非工作时段	邮件	<24 小时	
紧急、严重情况解决时间	工作时段	电话	<3 小时	
		邮件		紧急邮件
	非工作时段	电话	<5 小时	
		邮件		紧急邮件
非紧急、严重情况解决时间（服务请求）		电话	<72 小时（工作日）	
		邮件		
月度服务报告			每月初前 5 个工作日内发送上一月度报告	

7 数据中心机房要求

数据中心远离无线电干扰、强力电源，避开地震区和其他震源，避开环境污染区，远离容易发生燃烧、爆炸、洪水和低凹地区，远离高速公路主干道。

有良好的市政和生活配套设施，能够提供电力、通信等保障。

机房规模

根据项目目前实际情况和未来发展预计，投标人提供的数据中心需要一定规模，具备提供连续预留空间的能力。

建筑结构

抗震设防烈度：≥8度。

敷设防静电地板。地板承重≥800kg/㎡。

围护结构保温隔热，防火、电磁。

机房内部，设备运输通道畅通，保证本次项目设备妥善到达机房。

供电系统

双路供电，无单点故障隐患。

单路供电不小于16A的供电能力。

UPS采用2N冗余方式，每一路后备时间≥15分钟。

专用的柴油发电机组，保证机房全部负载不间断运行6小时以上。

后备发电机组功率>500KVA。

后备发电机组启动时间<10分钟。

发电机油料可以在2小时内获得补充。

机房不小于1KW/㎡的供电容量。

空调系统

采用N+1冗余模式，提供足够的制冷能力，并应留有20%的余量。

空调系统制冷量不低于1KW/㎡。

恒温、恒湿，常年温度 23±1 ℃，常年湿度 40%~55%。

空调机组下方装有拦水坝、漏水检测与报警系统，配备空调监控。

消防系统

消防中控室应配置有7*24小时值班人员，实时监控火灾自动报警系统。

机房需要配备便携式灭火器。

机房的安全出口应不少于两个，并设在机房的两端。机房门应向疏散方向开启，走廊、楼梯间应畅通并有明显的疏散指示标志。

安保系统

具备完善配套的环境监控系统。

机房闭路电视系统要求图像清晰。

监控录像至少保留一个月。

提供安全和可审计的门禁管理系统,电子门禁系统要求可设置不同权限。

7*24小时人员、设备进出管理服务。

7*24小时关键区域、出入口保安值班。

有登记制度和记录备查。

7.1 数据中心机房运营服务需求

投标人需为采购人提供专业运营管理团队和运营管理服务，为采购人提供高质量高安全的数据中心运营管理服务；保证采购人在机房安排专职机房运行管理人员负责配电、温度、湿度、通风、安全、消防以及网络等设施7*24小时监控，

保证机房安全稳定运行；巡检间隔不超过4小时，并有日志记录。

投标人需为采购人提供7*24小时技术支持服务；提供7*24小时的客服热线；

投标人应指派专人对提供给采购人的服务进行跟踪和监测。

在数据中心，投标人为采购人提供系统维护时所必要的工作场所、技术支持和后勤保障服务。

当投标人所提供服务由于自身出现问题时，投标人须在30分钟内通知采购人，当故障修复时间大于2小时时，须告知采购人应急事件处置方法及事件处置进展，并在3个工作日内提交事件报告。

投标人在机房现场需要有必要的运维技术支持人员，在特殊情况下，能够为采购人提供必要的技术支持服务。

7.2 其他要求

★如采购人现有硬件、信息系统及基础数据需要进行迁移，投标人应组织相关技术人员（含第三方软、硬件承建商人员）24小时内配合采购人完成现有硬件、信息系统及基础数据的迁移，并确保采购人硬件、信息系统及基础数据运行的连续性与完整性。（提供加盖投标人公章的承诺函）

8 履约验收要求

（1）隐私保密要求：投标人应严格遵守保密法律法规和规章制度，履行保密义务。不以任何方式向第三方泄露或传播本次项目相关内部数据及技术信息。

（2）验收方法：本项目按招标文件要求完成所有工作任务后，进行项目总验收。验收工作由中标人提出，采购人组织相关人员组成评审组进行验收。

（3）验收时间：云存储服务按招标文件要求实施，并稳定运行一个月后，由中标人提出验收申请，采购人应于中标人提出验收申请后十个工作日内组织云平台资源验收。采购人验收合格后应当出具验收报告。云平台服务期满前一个月采购人组织进行云平台服务验收。

（4）验收内容：按照招标文件、投标文件、合同、相关承诺和相关补充文件的内容进行。

（5）验收标准：云存储服务所有技术性能规格及参数应符合招标文件和中标人投标文件所要求的技术标准及服务标准。系统运行稳定，无故障，数据无错误。

（6）验收文件的签署：由中标人撰写服务完成报告，由采购人委派的负责

人在审核后签署。

四、商务要求

序号	商务条款	内容
1	★服务期	一年（2026 年 1 月 1 日至 2026 年 12 月 31 日），服务期满后，根据服务质量考核结果，采购人可以选择续签服务合同，续签合同最多不超过 2 年。
2	★服务地点	武汉市东西湖区公共资源交易中心
3	★报价要求	（1）投标人的报价应包含为完成本采购文件提出的云存储服务及相关的网络接入、数据迁移（如有）、安全防护、运维服务等全部相关工作所有可能发生的费用，即总报价为“交钥匙”价。对在合同实施过程中可能发生的其他费用（如：材料涨价、人工、运输成本增加等因素），采购人概不负责。 （2）对于本文件未列明，而投标人认为必需的配套产品费用应包含在投标总报价中，在合同实施时，采购人将不再支付额外费用。
4	★付款方式	云平台资源交付验收后支付合同金额的 40%，云平台服务期满前一个月进行云平台服务验收，验收后 60 日内支付合同金额的 60%。