2023-2024年度武汉市政府网站集约化平台基础资源及安全运维服务采购需求

一、采购背景

为延续武汉市政府网站集约化平台（以下简称“平台”）作为全市政府网站基础底座的支撑作用，确保全市政府网站安全稳定运行，拟通过购买服务采购平台基础资源和安全运维服务，保障全市政府网站管理效能、服务效率和社会效益，打造更加全面的政务公开平台、更加权威的政策发布解读和舆论引导平台、更加及时的回应关切和便民服务平台。

二、服务期限

自合同签订之日起到项目服务期满（365个日历天）

三、采购内容

序号	名称	数量	单位
1	平台技术运维服务	1	套
2	云资源及链路租赁服务	1	套
3	平台安全服务	1	套
4	监测与抽查服务	1	套

四、采购要求

本项目在延续前期运维服务基础上，以购买支撑平台持续安全运行的基础资源及安全运维服务为保障，各供应商需提供详细的投标方案并承诺所提供的方案都是真实、有效、合法的，必须完全满足采购人的采购需求，并确保平台运维交替期安全稳定运行。合同签订后，

供应商必须先行投入投标方案中所需基础资源服务，并经审核确定平台投入正常运行后，采购方开始计算项目服务期并支付服务费用。如果所提供的资源无法确保平台稳定运行的，采购人有权以供应商虚假承诺为由终止合同并要求供应商赔偿。

（一）平台技术运维服务要求

根据国家、湖北省和武汉市政府网站和平台建设发展需要，保障平台安全稳定运行，不断完善平台功能，优化提升服务水平，为全市各区、各部门政府网站提供更有力支撑。包括但不限于网站集约化平台、统一信息资源库、数据集约与对接服务、与省集约化平台对接联动等技术运维服务，具体要求如下：

1、平台功能技术支持：提供平台整体软件环境、资源部署的技术运维。包括但不限于站点管理、栏目管理、信息采编发布、模板管理、用户和组织管理、政府信息公开、互动信箱、在线调查、在线访谈、评论中心、意见征集、智能搜索等模块的功能巡检、配置调整、优化升级，确保平台所有功能模块7×24正常运行。同时，根据采购用户要求对入驻平台的所有网站提供技术支持、问题咨询和应急响应等各项技术服务。

2、对平台进行定期或不定期巡检：服务器运行状况、存储空间状况、软件运行状况、硬件运行状况、备份系统状况等。并提出现有问题和解决方法，及时发现和排除潜在问题或故障隐患，保证系统的稳定运行。（基于应用软件的系统运行日志、服务器的运行监控软件、数据库日志等多种方式进行运行状况的检查）。

3、运行环境的性能排查：对平台部署的各服务器运行状况、存储空间状况、软件运行状况、备份系统状况等方面进行常态化检查，包括：web 服务器等中间件协同配置检查与优化；系统基本配置情况，包括 CPU、内存等情况；网络问题的排查，包括数据库服务器和应用服务器之间的网络情况，客户端与应用服务器之间的网络情况等；访问较慢页面排查；文件目录的冗余处理；数据库的运行情况，数据库的冗余处理等服务。

4、平台升级：集约化平台版本迭代更新升级服务。

5、网站性能优化：定期对市政府网站 web 应用做优化服务，以提升网站的运行性能。

6、系统故障维修和产品升级：及时处置平台和各政府网站使用过程中的故障、系统安全、系统漏洞、第三方等保评测、安全补丁修复等；对第三方提出的安全报告及时调整处理，并对事件处理全流程进行跟踪监督，确保相关问题得到及时的响应与处理。接到报障通知后，须在 10 分钟内通过电话等方式响应回复，并在 2 小时内解决故障，故障排除后 3 个工作日内提交《故障处理报告》。在服务期内，技术支持人员免费提供产品升级服务，并对系统存在的问题进行修补或更新开发。

7、应急保障：提供重保或节假日期间 7×24 小时值班备勤服务，包括但不限于现场、远程等支持方式，并按照采购人要求提供技术人员现场驻场值守驻场和其他保障等服务。

8、搜索服务优化：持续优化相应的功能，提高平台工作效率。

9、网站“一号登录”优化：根据反馈，结合用户新需求，对网站“一号登录”进行功能和性能优化。

10、全文检索模块优化:根据反馈，结合用户新需求，对全文检索模块进行功能和性能优化。

11、互动模块优化:根据反馈，结合用户新需求，对网民互动模块进行功能和性能优化。

12、其它类服务：根据采购人需求，完成平台各类对接、应用性调整和突发性技术支持等服务。

（二）云资源及链路租赁服务要求（详见附件 1）

1、云主机技术要求

（1）云主机支持整机备份，支持快照技术的备份服务，备份数据恢复到原有服务器或新服务器。

（2）云主机支持在创建时支持设置多个网卡，并且可以设置不同的 IP 地址。

（3）云主机支持提供虚拟主机的动态升级、快照备份、异常告警、日志管理等功能；支持创建不同规格的虚拟主机，自定义 CPU、内存、网络、磁盘等属性。

（4）云主机支持计算能力的水平弹性伸缩。

2、云存储技术服务要求

（1）云硬盘技术要求：支持云主机共享盘，支持为云主机提供 SATA、SAS、SSD 类型的云硬盘；满足用户业务突然高峰性能需求,最大 IOPS 不小于 33000；支持 1 台云主机最多可挂载 16 块云硬盘。

（2）海量数据存储服务要求。支持访问控制功能，可以设置基于用户和用户组的策略，并将策略授权给用户和用户组，精确控制用户和用户组对指定服务和资源的访问权限；支持同一存储服务中可以同时提供块、文件和对象三种多协议存储服务；服务设计可用性不低于99.95%，数据设计持久性可高达99.9999999%。

3、云机房服务要求

（1）投标人拥有自有产权云机房，且达到国标A级机房标准，需提供机房权属证明。

（2）投标人可提供项目所在地其他云机房供选择，并完全满足如下要求：

投标人提供的候选云机房必须为IDC机房（可供现场考察），并具备容灾机房能力（国境内，与候选云机房不在同一地点），满足应急故障情况容灾。

所有候选机房使用要求，需满足以下任意一条：

（1）候选机房为投标人自有产权的，需提供机房权属证明。

（2）若候选机房为租用机房的，投标人需提供相关租赁材料或者承诺在中标后本项目合同用户规定时间内租用到使用的机房。

4、链路服务要求

（1）需提供两条500M互联网接入服务。两条线路共包含128个互联网IPv4和IPv6地址，并提供技术方案，证明能和原IP地址平滑过渡。

（2）需要提供一条1000M政务外网接入服务。包含256个政务外网IPv4地址，并提供技术方案，证明能和原IP地址平滑过渡。

（三）云安全服务要求（详见附件2）

满足等级保护2.0三级“一个中心、三重防护”标准，基于平台运营过程中的实际安全需求，构建平台独享网络安全保障体系。对平台、网站、链路及支撑环境提供合规的、全面的、自主可控的安全服务，包含且不限于：防火墙服务、主机安全防护服务、入侵防御服务、数据库安全审计服务、运维审计服务、应用安全防护服务、应用安全基础服务、应用系统威胁捕获服务、综合安全监控分析服务、网页防篡改服务、互联网安全服务、日志审计服务、Ipv4/IPv6支持服务、应急保障服务等。健全平台综合安全监控中心，基于全量网络流量、威胁检测、运维响应、资产管理、SOAR、威胁事件和终端日志等进行智能化数据汇聚分析，提供平台各项安全监测指标数据的实时汇聚、人工分析研判及预警通告等服务保障，具备对平台运行环境、动态、整体地呈现全局安全风险实况，实现整体安全威胁的可知、可视、可控，确保平台运行稳定、安全可靠。

（四）监测与抽查服务要求

通过监测与抽查服务，面向全市正常运行中的政府网站进行全面监测，每月进行监测，每个季度进行抽查，通过对各政府网站进行全天24小时系统监测以及定期人工监测相结合的形式，及时发现网站存在的突出问题并及时整改实现全市政府网站的整体达标。

1、月度监测服务：每月需提供可用性检测服务；网站严重表述错误检测服务；网站无效链接监测服务；网站暗链、伪链监测服务；网站涉密、涉敏信息监测服务。

2、季度抽查服务：每个季度需提供自动监测、人工监测、多渠道预警机制服务内容，并出具季度抽查报告。

五、其他要求

（一）服务方式

中标供应商提供7×24通过远程、上门服务、电话、E-mail等方式为用户提供相关技术咨询服务。

（二）人员要求

投标人拟投入运维服务人员不得低于10人，服务小组成员须具备相应技术资质，包括但不限于如下人员：服务小组成员之一具PMP资格或其他同等资格；服务小组成员之一具备CISP（注册信息安人员）资格。

（三）验收要求

本项目严格按照政府采购相关法律法规以及《财政部关于进一步加强政府采购需求和履约验收管理的指导意见》（财库〔2016〕205号）的要求进行验收。

验收步骤：

1、项目初验：项目初验为所提供整体资源能够投入正常使用的验收。

中标供应商应按照采购人要求，提供满足采购人需求的全部资源能够投入正常使用且运行平稳后，由监理服务商开展检测核查，经采购人审查并达到采购需求的为完成项目初验，项目进入运维服务期。

2、项目终验：项目终验为项目运维服务到期后整体完成情况的验收。

中标供应商所提供的各项服务即将到期时，中标供应商向监理服务商提请项目终验申请，采购人按照合同要求及验收程序组织最终验收。供应商应将服务期间的平台运维服务文档、云资源及安全运行维护资料等文档汇集成册交付采购人，缺一不予验收。

（四）技术服务要求

运维期内应提供现场及远程技术维护方案，由中标方负责对云资源及链路功能完善、应急响应和产品升级，期间如发生系统运行故障或出现瑕疵与缺陷的，中标供应商需及时作出响应，并提供相应解决方案。

（五）保密要求

在运维期内中标供应商负责的服务工作，中标供应商必须严格遵守采购人各项管理规定，并签订保密协议。在任何情况下，禁止复制、传播、引用及非开发需要查询所接触到的采购人各类业务数据、工作要求和工作措施等信息；未经授权禁止向采购人主管部门以外的单位和个人演示该系统，采购人保留追究法律责任的权力。

（六）培训要求

投标人应针对集约化平台管理员人员、全市各政府网站相关管理员人员提供相应的技术培训，投标时须提供相关材料。

（七）报价要求

1、供应商报价应包含人工费、通讯费、交通费等完成本项目的所有费用。因供应商自身原因造成漏报、少报皆由其自行承担责任，采购人不再补偿。

2、云资源租赁不得高于2023年市直各部门和单位采购政务云服务的单价。

3、供应商报价不超过376.86万元，超过采购预算的，其报价无效。

4、签订合同时另行约定。

附件1：云资源及链路服务资源

1、云主机					
序号	**服务项目**	**服务说明**	**计费单位**	**数量**	**备注**
1	云主机	vCPU≧8核、内存≧16GB	台/年	20	免费操作系统
2	云主机	vCPU≧16核、内存≧16GB	台/年	36	
3	云主机	vCPU≧16核、内存≧32GB	台/年	10	
4	云主机	vCPU≧32核、内存≧64GB	台/年	6	
合计				72	
2、云存储					
序号	**服务项目**	**服务说明**	**计费单位**	**数量**	**备注**
1	云硬盘	高速云硬盘	GB/年	108600	
2	云备份	用于云平台数据的本地备份存储	1TB/年	10	
3、网络通信					
序号	**服务项目**	**服务说明**	**计费单位**	**数量**	**备注**
1	互联网带宽	两条500M互联网链路	500M/年	2	
2	电子政务外网	1000Mbps电子政务外网专线	1000M/年	1	免费提供
3	电子政务外网IP	电子政务外网IP	个/年	≥254	
4、其它服务					
序号	**服务项目**	**服务说明**	**计费单位**	**数量**	
1	短信服务	短信服务套餐（50万条/年）	套/年	1	
（注：供应商所投入基础资源不得低于以上内容，并提供相关证明材料。）					

附件 2：云安全服务清单

序号	服务项目	服务说明
1	防火墙服务	包括但不限于提供防火墙吞吐量≥10G，最大并发连接数≥1000万，每秒新建连接数≥16 万，包含 100 个 SSLVPN 授权服务。具备容器化服务能力,对 NAT 地址池中的地址进行有效性探测服务，在出现地址池地址不可用的时候自动排除，保障互联网业务安全稳定运行。支持动态负载均衡技术采用自适应创新链路选择控制算法，可实时主动探测链路的连通状况、延迟情况及抖动，形成智能闭环，以便根据当前时刻的链路状况作出最优选路。支持嵌套式流控功能服务能力，具备至少两个维度的流量控制。上述功能需提供相关功能截图或证明文件复印件，并加盖原厂公章。
2	主机安全防护服务	包括但不限于提供专业主机安全防护服务，针对服务器物理机、虚拟机和容器环境提供一站式安全防护能力，支持自动获取主机信息，主机信息包括硬件类型，操作系统版本，系统内核版本，CPU 数量，内存，主机 IP 等。提供微隔离功能服务，支持主机与主机之间的网络访问，外部地址与主机之间访问，部署微隔离策略。上述功能需提供相关功能截图或证明文件复印件，并加盖原厂公章。
3	入侵防御服务	包括但不限于提供专业入侵检测系统，支持多重威胁检测和防御能力，支持对僵尸网络攻击、DDoS 攻击、已知协议漏洞利用、Web 攻击、垃圾邮件、钓鱼、木马病毒和恶意软件等一系列网络入侵威胁进行检测及防御。上述功能需提供相关功能截图或证明文件复印件，并加盖原厂公章。
4	数据库安全审计服务	包括但不限于提供采用精准协议解析、海量日志存储和检索等技术，通过对访问数据库的行为、内容等进行采集、存储、分析，实现完全独立于数据库的审计功能服务，一套系统内即可同时支持包括数据库审计、数据库防火墙、数据脱敏、风险扫描、状态监控、运维审计等功能。上述功能需提供相关功能截图或证明文件复印件，并加盖原厂公章。
5	运维审计服务	包括但不限于提供运维管理和运维安全融合服务，通过身份认证、权限控制、账户管理、操作审计等多种手段，完成对资产的统一认证、统一授权、统一审计，全方位提升运维风险控制能力。满足任意浏览器播放审计日志视频回放、监控、切断；所有审计日志以会话为单位，支持完整回放；正在连接中的会话支持实时监控与阻断。同时加载水印在播放页面。上述功能需提供相关功能截图或证明文件复印件，并加盖原厂公章。
6	应用安全防护服务	包括但不限于提供 web 应用安全防护，采用深层代理、应用漏洞扫描、日志聚合、智能自学习等多项技术，从 TCP Option 获取源 IP 地址（TOA）、支持移动运维与“一键应急断网功能服务”、用户会话跟踪功能的服务；支持攻击检测双引擎，即语义解析引擎 + 规则防护引擎，语义解析引擎通过词法分析、语法分析及语义分析对报文进行检测。上述功能需提供相关功能截图或证明

		文件复印件，并加盖原厂公章。
7	应用安全基础服务	包括但不限于提供全方位的系统扫描检查和安全评估，协助管理者高效、准确的对内部系统进行实时自检，以针对性提升网络的整体安全性。本次服务所用工具，支持与态势感知服务工具联动，进行全网脆弱性分析。上述功能需提供相关功能截图或证明文件复印件，并加盖原厂公章。
8	应用系统威胁捕获服务	包括但不限于提供模拟不同类型的服务，并在设置一些常规漏洞，诱骗攻击者利用漏洞对其实施攻击，触发攻击告警，继而进行攻击溯源并做及时处置，有效防止攻击者在内网中横向扩散。上述功能均需提供相关功能截图或证明文件复印件，并加盖原厂公章。
9	综合安全监控分析服务	包括但不限于聚合从威胁探针、防火墙、应用安全防护、应用安全基础等服务的流量和日志数据，实现全网流量安全分析。自动识别流量中常见的应用协议，并按照应用维度进行流量统计与分析。支持的应用协议包含不限于 RDP、SSH、HTTP、SNMP、FTP-DATA、微信文件传输、UDP 下载及视频等至少 5000 种以上的应用协议；支持按照 IP 地址、通讯协议、端口等自定义应用识别规则。提供自动化编排响应剧本服务，实现全网联防联动，快速检测出问题并下发处置动作到联动设备（防火墙、WAF 等），作出及时响应，并形成相应的安全任务，通过邮件、短信等方式推送给对应的管理员。提供以图形展示每个终端在不同时期的流量数据情况的服务能力，包括但不限于，目的 IP、目的端口、服务、基线学习状态。提供重保工作台：包括实时告警、溯源模式、一键阻断、重保报告、重保配置助手功能模块；提供挖矿专项服务：展示挖矿阶段分布、挖矿币种分布、挖矿资产 Top5、受害资产列表及详情，支持筛选、导出、批量标记、加白及处置等操作。防勒索专项：展示勒索阶段分布、勒索事件分布、受勒索资产 Top5、受害资产列表及详情，支持筛选、导出、批量标记、加白及处置等操作；弱密码专项：展示弱密码 Top20、主要弱密码事件、弱密码目的 IP Top5、弱密码清单列表及详情，支持筛选、导出等操作。提供基线学习结果作为流量异常检测依据，如出现异常流量，会进行异常流量告警。上述功能均需提供相关功能截图或证明文件复印件，并加盖原厂公章。
10	网页防篡改服务	包括但不限于提供基于内核驱动级文件保护技术，支持各类网页格式，包含各类动态页面脚本；支持大规模连续篡改攻击防护；支持断线状态下阻止篡改；完全杜绝被篡改内容被外界浏览；支持单独文件、文件夹及多级文件夹目录内容篡改保护保护站点内容安全，防止黑客非法篡改网页，保护公众形象。系统通过服务器文件访问底层驱动技术，对保护的对象(静态网页、动态执行脚本、文件夹)实时监测其属性。上述功能均需提供相关功能截图或证明文件复印件，并加盖原厂公章。
11	互联网安全服务	包括但不限于提供互联网线路的互联网安全配套服务。服务内容为对客户的网站域名提供防篡改服务，对互联网流量提供抗 D 攻击保护和流量清洗服务。实时流量监控和全面风险评估，当流量

		出现异常或者超过预先设置的阈值时可启动防护清洗，并与攻击结束后及时提供攻击报告。上述功能均需提供相关功能截图或证明文件复印件，并加盖原厂公章。
12	日志审计服务	包括但不限于提供日志审计服务，实现网络日志的集中采集、分析挖掘、合规审计、实时监控及安全告警、报表生成等，可关联策略产生审计事件、如时间、IP 地址、方式等，对于相符合的结果，系统将在关联事件中呈现，并为用户提供自定义日志查询功能服务。上述功能均需提供相关功能截图或证明文件复印件，并加盖原厂公章。
13	Ipv4/IPv6 支持服务	包括但不限于采用 IPv6 反向代理功能，进行 IPv4 到 IPv6 的转换，实现使用 IPv6 的公网资源访问集约化系统的内部站点。支持用户通过 IPv4/IPv6 双协议访问并获取服务，同时进行安全性加固。上述功能均需提供相关功能截图或证明文件复印件，并加盖原厂公章。
14	网站证书服务	包括但不限于提供平台承载全部网站（满足等保要求）HPPTS 证书，通过传输加密和身份认证方式保证传输过程的安全性。上述内容均需提供相关功能截图或证明文件复印件，并加盖原厂公章。
15	应急保障服务	包括但不限于在特殊时期、重要活动、重大节假日，提供合规专业安全工具或人员对平台系统、应有软件、数据库和中间件、等相关体系进行全面与深度安全检测，并对发现的问题及时修复加固。且具有应急响应处置、安全事件溯源的服务能力，并派遣专业安全事件应急服务人员协助分析或上门处置等相关服务。每年至少组织 1 次安全演练，并提供演练报告。