**采购需求**

1. **采购项目情况**

**（一）项目基本情况**

1.项目名称：\_北京市文化市场综合执法总队2025年信息系统政务云基础资源租用服务项目\_\_\_

2.项目预算金额：\_259.07\_万元

3.采购包情况：

|  |  |  |  |
| --- | --- | --- | --- |
| 包号 | 标的名称 | 采购包预算金额  （万元） | 数量 |
| 01 | 北京市文化市场综合执法总队2025年信息系统政务云基础资源租用服务项目 | 259.07 | 1 |

4.合同履行期限：\_12个月，从2025年3月10日至2026年3月9日\_\_

5.本项目是否接受联合体投标：□是 ☑否。

1. **规范性引用文件**

**（一）国家及北京市有关政策**

1.《关键信息基础设施安全保护条例》（中华人民共和国国务院令第745号）

2.《国家政务信息化项目建设管理办法》（国办发〔2019〕57号）

3.《政府采购需求管理办法》(财库〔2021〕22号)

4.《关于促进政府采购公平竞争优化营商环境的通知》（财库〔2019〕38号）

5.《关于进一步提高政府采购透明度和采购效率相关事项的通知》（财办库〔2023〕243号）

6.《工业和信息化部信息通信管理局关于督促互联网网络接入服务企业依法持证经营的通知》（工信管函〔2018〕84号）

7.《云计算服务安全评估办法》（国家互联网信息办公室、国家发展和改革委员会、工业和信息化部、财政部公告2019年2号）

8.《关于加强党政部门云计算服务网络安全管理的意见》（中网办发文〔2014〕14号）

9.《基于云计算的电子政务公共平台顶层设计指南》

10.《北京市财政局关于印发<北京市政府采购负面清单>的通知》（京财采购〔2020〕1345号）

11.《北京市财政局关于落实好政府采购支持中小企业发展的通知（京财采购〔2022〕1143号）

12.《关于印发<关于推进我市政务信息系统整合共享的实施方案>的通知》（京经信委发〔2017〕89号）

13.《北京市人民政府关于印发<北京市政务信息资源管理办法（试行）>的通知》（京政发〔2017〕37号）

14.《关于印发<北京市市级政务云管理办法>的通知》（京经信函〔2019〕150号）

15.《北京市政务网络和数据安全管理办法》（京经信发〔2023〕57号）

16.《北京市“十四五”时期智慧城市建设控制性规划要求（试行）》（京大数据发〔2021〕2号）

**（二）国家相关标准**

1. 《国家电子政务外网安全接入平台技术规范》
2. 《信息技术—云计算—云服务质量评价指标》（GB/T 37738-2019）
3. 《信息技术—云计算—云服务计量指标》（GB/T 37735-2019）
4. 《信息技术—云计算—云服务采购指南》（GB/T 37734-2019）
5. 《信息技术—云计算—云存储系统服务接口功能》（GB/T 37732-2019）
6. 《信息技术—云计算—云资源监控通用要求》（GB/T 37736-2019）
7. 《信息技术—云计算—云平台间应用和数据迁移指南》（GB/T 37740-2019）
8. 《信息技术—云计算—云服务交付要求》（GB/T 37741-2019）
9. 《信息系统灾难恢复规范》（GB/T 20988-2007）
10. 《信息安全技术 云计算服务安全能力要求》（GB/T 31168-2014）
11. 《信息安全技术 网络安全等级保护定级指南》（GB/T 22240-2020）
12. 《信息安全技术 网络安全等级保护基本要求》（GB/T 22239-2019）
13. 《信息安全技术 网络安全等级保护测评要求》（GB/T 28448-2019）
14. 《信息安全技术 信息系统密码应用基本要求》（GB/T39786-2021）
15. 《信息安全技术 信息安全风险评估方法》（GB/T 20984-2022）
16. 《信息安全技术 云计算服务安全指南》（GB/T 31167-2014）
17. 《信息安全技术 政府网站云计算服务安全指南》（GB/T 38249—2019）
18. 《信息安全技术 云计算安全参考架构》（GB/T 35279—2017）
19. 《信息安全技术 云计算服务安全能力评估方法》GB/T 34942—2017
20. 《信息安全技术 云计算服务运行监管框架》（GB/T 37972—2019）
21. 《信息技术 云资源监控指标体系》（GB/T 37938-2019）
22. 《电子信息系统机房设计规范》（GB50174-2017）
23. 《数据中心电信基础设施标准》（ANSI/TIA-942）
24. 《综合布线系统工程设计规范》（GB 50311—2016）
25. 《云计算关键领域安全指南V4.0》

**（三）北京市相关标准**

1. 《政务云平台建设技术要求》（DB11/T 2169-2023）
2. 《北京市政务云安全技术规范 IaaS云计算平台分册》
3. 《北京市政务云安全技术规范 IaaS云计算平台安全监管接口分册》
4. 《北京市政务云安全技术规范 信息安全服务接口分册》

**（四）其他**

1. 《北京市市级行政事业单位云计算服务框架协议采购项目（2023 年度）》征集文件第四部分采购需求中技术要求

**注：服务标准涉及的国家标准及北京市标准有更新的，执行最新标准。**

1. **项目背景或概况**

北京市文化市场综合执法总队（简称市文化市场执法总队），为市委宣传部、市文化和旅游局双重管理的副局级行政执法机构，以市文化和旅游局名义执法。 （一）负责集中行使法律、法规、规章规定的文化、文物、新闻出版、版权、广播电视、电影、旅游市场以及宗教等领域应由省级行政主管部门行使的行政处罚权以及与之相关的行政检查、行政强制权。 （二）负责相关领域重大疑难复杂案件和跨区域案件的查处工作。 （三）负责指导、协调、监督、考核各区文化市场综合执法工作。 （四）承担“扫黄打非”有关工作任务。 （五）完成市委、市政府和市委宣传部、市文化和旅游局交办的其他任务。

本项目将为支撑文化市场执法总队信息化系统和平台提供政务云服务。

1. **技术参数要求**

**（一）政务云基础服务**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **服务子类** | **服务项** | **计价单位** | **报价单位** | **数量** | **服务期（月）** |
| x86平台云主机服务 | vCPU（主频不低于2.4GHz） | 1CPU | 元/月 | 768 | 12个月 |
| 内存 | 1GB | 元/月 | 1888 | 12个月 |
| 高性能存储 | 高性能存储（单盘技术指标：单盘IOPS3000-20000） | 1GB | 元/月 | 74560 | 12个月 |
| 备份服务 | 租用快照备份服务 | 1GB | 元/月 | 6930 | 12个月 |
| 互联网链路服务 | 互联网链路带宽 | 1Mb | 元/月 | 220 | 12个月 |
| 互联网IP地址租用服务、并提供备案服务 | 1IP | 元/月 | 15 | 12个月 |
| 主机负载均衡服务 | 主机负载均衡服务 | 1IP（内网） | 元/月 | 13 | 12个月 |
| 远程接入服务 | 远程接入服务 | 1账号 | 元/月 | 12 | 12个月 |
| WAF防护 | web应用防火墙服务 | 1IP（互联网） | 元/月 | 10 | 12个月 |
| VPN服务 | SSL VPN接入 | 1套 | 元/月 | 14 | 12个月 |

**（二）政务云扩展服务**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **服务类别** | **服务子类** | **服务项** | **计价单位** | **报价单位** | **数量** | **服务期（月）** |
| 基础软件支撑服务 | 商用操作系统套餐 | Windows Server套餐：Windows Server租用、安装及维护。 | 1套 | 元/月 | 18 | 12个月 |
| 国产操作系统服务租用、安装及维护。 | 1套 | 元/月 | 41 | 12个月 |
| 开源操作系统套餐 | 提供开源操作系统安装和维护服务。 | 1套 | 元/月 | 34 | 12个月 |
| 商用数据库套餐 | 国产商用数据库租用、安装及维护（至少支持3种国产数据库） | 1套 | 元/月 | 2 | 12个月 |
| 开源数据库套餐 | 开源数据库安装及维护服务 | 1套 | 元/月 | 9 | 12个月 |
| 办公软件服务 | 全终端兼容的文档协作云平台服务 | 1套 | 元/月 | 1 | 12个月 |
| 安全服务 | 云端抗DDOS服务 | 云端抗DDOS服务 | 1 站点 | 元/月 | 4 | 12个月 |
| 云端APT防护服务 | 云端APT防护服务 | 1 套 | 元/月 | 4 | 12个月 |
| 主机杀毒服务 | 主机杀毒服务 | 1台 | 元/月 | 101 | 12个月 |
| 其他服务 | 签名验证服务 | 签名验签、杂凑等密码运算服务 | 1项 | 元/月 | 1 | 12个月 |
| 加解密服务 | 为系统提供数据加解密服务 | 1项 | 元/月 | 1 | 12个月 |
| 时间戳服务 | 为应用系统提供安全、可信的时间戳服务 | 1项 | 元/月 | 1 | 12个月 |
| SSL安全服务（国密） | 提供基于SM2/3/4算法的SSL通信信道安全服务 | 1项 | 元/月 | 1 | 12个月 |

1. **采购目标**

本项目的总体目标是通过租用政务云平台基础服务，对总队信息化的运行环境进行持续支撑，提供可靠、稳定、安全的政务云基础服务，具体包括：

1. 提供政务云基础服务，包括计算服务、存储服务和网络服务等基础环境日常维护、应急响应等工作。
2. 提供7\*24运维保障，做好重大活动和节假日应急值守保障服务，确保各系统在政务云环境中可靠稳定运行。
3. 服务期内，投标人须完成信息系统的日常运维和安全运维服务工作（包括但不限于：云平台服务、日常技术支持、系统日常维护、服务规范、安全及保密要求、响应的及时性），确保入云系统安全、稳定的运行。
4. **服务内容与服务标准**

**（一）云主机服务**

**1.1服务内容**

按照采购人的具体需求，提供x86云主机服务，包括：768核vCPU和1888GB内存，按需求对CPU及内存进行动态调整，实现合理的计算资源配置。在提供政务云主机的服务过程中做好与采购人和对应项目应用开发厂商的协调沟通工作。

**1.2服务标准**

1.2.1云主机服务应按内存不复用方式分配资源，要求CPU主频≥2.4GHz,CPU核数可选范围1-16核，内存可选范围1-64G；

1.2.2云主机应支持主流操作系统，如windows server系列、Linux发行版、国产Linux等，需正版授权；

1.2.3 应具备扩展性，用户可以灵活调整云主机CPU、内存、硬盘规格；

1.2.4对不同用户的虚拟主机提供安全组和VLAN级别的隔离，确保不同用户之间数据互不可见；云主机之间可以做到隔离保护，其中每一个云主机发生故障都不会影响同一个物理机上的其它云主机运行，每个云主机上的用户权限只限于本云主机之内，以保障系统平台的安全性；

1.2.5 用户对云主机有完全的控制权，具有管理员权限，使用方式与传统物理主机完全一致；

1.2.6 虚拟化管理节点须支持双机热备，虚拟化管理系统支持虚拟机的HA功能，硬件设备出现故障时，云主机会自动进行HA切换；

1.2.7支持云主机备份功能，可以实现云主机的全量备份、增量备份，支持备份周期、备份策略的设定；

1.2.8支持通过云管理平台，实现申请部署与使用；

1.2.9 提供防ARP欺骗、自定义防火墙功能，支持防DDOS攻击；

1.2.10支持虚拟路由、虚拟交换机和弹性IP，用户可自定义虚拟主机的网络拓扑和IP地址；

1.2.11创建虚拟主机时，可指定用户预先配置好的镜像文件作为模板。虚拟主机支持增量快照备份功能，提高备份效率，减小备份占用空间，并支持公共镜像、私有镜像以及共享镜像等多种方式；

1.2.12虚拟主机底层采用分布式块存储，每个虚拟主机的镜像存储达到多副本可靠性，数据可靠性不低于99.9999%；

1.2.13虚拟主机服务采用全冗余架构，无单点故障，平均可用性不低于99.99%；

1.2.14支持计算能力的垂直伸缩，支持对CPU和内存的升级与降级操作，支持增加、减少磁盘和带宽；支持计算能力的水平伸缩，通过与负载均衡配合实现水平伸缩。

**（二）存储服务**

**2.1服务内容**

按照采购人的具体需求，提供74560GB的高性能存储服务。在提供政务云存储的服务过程中需做好采购人和对应项目应用开发厂商的协调沟通工作。

**2.2服务标准**

2.2.1 要求稳定可靠，不会因单一部件故障、单一路径故障等原因导致业务停用、数据丢失，系统可靠性99.9999%；

2.2.2 单盘技术指标满足IOPS 10000-25000；

2.2.3 用户可以以1G为最小单位进行容量申请，并可以申请直接挂载给云主机使用，同时用户可以将申请到的磁盘空间分配给一台或者多台虚拟机/物理机使用；

2.2.4 系统整体架构无单点故障；

2.2.5 支持通过云管理平台，实现申请部署与使用；

**（三）数据库服务**

无

**（四）网络服务**

**4.1服务内容**

4.1.1 提供220Mb的互联网链路带宽服务，提供15IP的地址租用服务，并提供相应的网络域名备案服务，配合应用开发厂商提供网络策略配置服务；

4.1.2 主机负载均衡服务，提供13IP的主机负载均衡服务，通过云管理平台实现针每租户按需自动分配负载均衡服务的能力；

4.1.3 远程接入服务，提供12账号的互联网远程接入服务，每个账号结合身份验证接入堡垒机维护应用系统；

4.1.4 VPN服务，提供14套SSL VPN接入服务；

4.1.5 WAF防护服务，提供10IP的WAF防护服务。

**4.2服务标准**

4.2.1 互联网链路服务应满足如下服务标准：

4.2.1.1具备多运营商网络接入服务的能力；

4.2.1.2 为平台业务系统提供互联网带宽租用服务；

4.2.1.3 支持通过云管理平台，实现申请部署与使用；

4.2.1.4 可提供IPV4/IPV6互联网IP 地址租用服务；

4.2.1.5 配合使用单位完成网站域名备案；

4.2.1.6 支持通过云管理平台，实现申请部署与使用。

4.2.2 主机负载均衡服务应满足如下服务标准：

4.2.2.1 通过云管理平台实现针每租户按需自动分配负载均衡服务的能力。总体峰值可支持每秒新建链接数不少于40万；

4.2.2.2 支持加权轮询(Weighted Round Robin)、加权最小连接数调度(Weighted Least-Connection Scheduling)等流量分发策略；

4.2.2.3 可以按照指定规则对配置的虚拟主机进行健康检查，自动隔离异常状态虚拟主机，确保可用性；

4.2.2.4 可对虚拟主机提供TCP/HTTP协议的负载均衡服务，并提供会话保持功能，在会话生命周期内，将同一会话请求转发到同一台后端虚拟主机；

4.2.2.5 采用全冗余或集群架构，无单点故障；平均可用性不低于99.99%；

4.2.2.6 提供多种转发规则，满足不同业务场景的要求；

4.2.2.7 支持在线平滑升级，承载能力和网络总带宽同步线性扩容；可与虚拟主机配合提供三层架构系统的弹性扩展；

4.2.2.8 支持通过云管理平台，实现申请部署与使用；

4.2.2.9 提供 4 层（TCP 协议）和 7 层（HTTP 和 HTTPS 协议）的负载均衡服务。

4.2.3 远程接入服务应提供堡垒机远程接入服务，提供字符操作审计、图形操作审计、文件操作审计服务，应支持基于IP/IP段、用户/用户组、资产/资产组、协议、危险级别等组合策略进行访问控制，对于不合法的行为予以阻断；可基于运维账号的登陆时间和资产登陆时间进行访问控制；可基于运维操作命令进行访问控制；可基于主机、用户、IP地址控制审计日志的访问权限；

4.2.4 SSL VPN接入须实现Web接入，TCP接入，IP接入等多种方式，记录完整的用户访问日志；支持基于用户身份的管理，实现不同身份的用户拥有不同的命令执行权限，并且支持用户视图分级，对于不同级别的用户赋予不同的管理配置权限；可以根据请求报文的目的IP地址和目的端口号、源IP地址和源端口号进行过滤；采用通过商用密码产品认证的SSL VPN产品。

4.2.5 远程接入服务支持基于IP/IP段、用户/用户组、资产/资产组、协议、危险级别等组合策略进行访问控制，对于不合法的行为予以阻断；可基于运维账号的登陆时间和资产登陆时间进行访问控制；可基于运维操作命令进行访问控制；可基于主机、用户、IP地址控制审计日志的访问权限。

4.2.6 WAF防护服务可精确识别包括注入、XSS等OWASP Top 10 WEB通用攻击，有效应对盗链、跨站请求伪造等WEB特殊攻击；可以通过透明串接或反向代理、路由模式等方式接入网络中，即可对应用层HTTP流量进行安全防护；通过预定义策略及自定义规则，进行规则匹配，阻断异常流量；支持通过云管理平台，实现申请部署与使用。

4.2.7供应商应强化远程运维管理，因业务确需通过互联网远程运维的，应当采取安全管控措施，向采购提供安全管控方案。重要保障时期避免通过互联网远程运维。

**（五）基础软件支撑服务**

**5.1服务内容**

按照采购人的有关管理规定及具体需求，提供18套商用操作系统、41套国产化操作系统、34套开源操作系统、2套国产商用数据库、9套开源数据库、1套办公软件服务。

**5.2服务标准**

5.2.1商用操作系统套餐

提供主流商业操作系统服务，应支持Windows Server操作系统的各种主流版本，并提供操作系统的安装部署和各种故障处理。

5.2.2 国产化操作系统

提供主流国产化操作系统服务，应支持银河麒麟、中标麒麟、统信等主流操作系统的各种版本，并提供操作系统的安装部署和各种故障处理。

5.2.3 开源操作系统套餐

提供主流开源操作系统服务，应支持Ubuntu等主流Linux操作系统的各种版本，并提供操作系统的安装部署和各种故障处理。

5.2.4 国产化数据库套餐

提供主流国产商用数据库服务，应支持3种以上（达梦、人大金仓、K-DB）国产数据库单机、集群的主流版本，提供数据库的安装部署和各种故障处理及日常维护。

5.2.5 开源数据库套餐

提供主流开源数据库服务，应支持MYSQL数据库的主流版本，提供数据库的安装部署和各种故障处理及配置优化，提供数据库日常维护。

5.2.6办公软件服务

提供全终端兼容的文档协作云平台服务，支持主流的办公软件服务，包括支持WPS文档在线预览、在线编辑、格式转换、内容处理等二次开发能力，如支持协同编辑、插入红头签章以及文档在线预览等能力，并兼容主流信创环境，让用户能够随时随地在云端进行文档协作，改善用户文档的操作体验。

**（六）资源调度服务**

**无**

**（七）安全服务**

**7.1服务内容**

安全是政务云的红线，应按照网络安全等级保护、关键信息基础设施保护、个人信息保护及数据安全保护等要求建设安全技术防护体系和安全管理体系，加强数据的安全管理，采用分级方式进行重点数据保护，防止重要或敏感数据泄露或被滥用，并建立应急处置体系，强化各领域平台安全管控，在深化数据融合应用的同时保障安全。须提供安全服务包含：4站点的云端抗DDOS服务、4套云端APT防护服务、101台主机杀毒服务。具体如下：

7.1.2云端抗DDOS服务

按照采购人的具体需求，根据流量提供云端抗DDOS服务，为云内应用系统抵御大流量分布式拒绝服务攻击。在提供服务的过程中需做好与采购人和对应项目的应用开发厂商的协调沟通工作。

7.1.3 云端APT防护服务

按照采购人的具体需求，提供云端APT防护服务，对未知攻击威胁进行检测和防护，发现隐蔽威胁、木马后门等异常威胁。通过APT防护服务，实现恶意代码检测、恶意软件检测及攻击溯源。

7.1.4 SSL安全服务（国密）

提供基于SM2/3/4算法的SSL通信信道安全服务，保证用户访问系统以及重要数据传输过程中的机密性和完整性。

7.1.5 主机杀毒服务

提供主机杀毒服务，通过杀毒软件，对云主机进行定期的病毒查杀，杀毒软件集中控制。

**7.2服务标准**

7.2.1 投标人所提供云平台应符合国家及行业标准、规范。政务云平台应参照《信息安全技术 网络安全等级保护基本要求》（GB/T22239-2019）第三级安全要求进行建设。

7.2.2 在单一云平台内部，政务投标人需要实现不同用户间业务应用系统及数据的安全隔离。

7.2.3 投标人应建立政务云平台应急管理体系，定期开展应急演练工作，保障灾难发生时，及时协助市文化市场执法总队开展系统应急工作，恢复系统及数据。

7.2.4 投标人应建立政务云平台重要时期安全保障体系，保障市文化市场执法总队政务信息系统在重要时期安全、稳定运行。

7.2.5 投标人应遵守市文化市场执法总队关于个人数据、敏感数据、重要数据保护、隐私保护相关规定，未经允许不得对云平台上的任何数据进行非法截取、加工、分析处理，严禁信息泄露给任何单位和个人。

**（八）运维服务**

**8.1服务内容**

8.1.1 负责机房环境资源、云平台硬件资产、虚拟化资产的管理工作；

8.1.2 信息系统入云、上线、变更、退出等各阶段的备案与信息变更等工作；

8.1.3 执行云平台变更申请、审批流程；

8.1.4 云平台网络资源管理，针对内部地址使用情况、云平台专线接入情况、政务外网资源使用情况等做好统计工作；

8.1.5 服务期内，投标人须配备运维团队，提供可靠的售后服务保障。投标人针对采购人要求的云平台运维服务相关内容，需指定专业技术能力较强的工程师，根据采购人要求配合开展相关维护服务。

**8.2服务标准**

8.2.1 提供技术服务热线(7\*24小时) 负责解答政务云平台使用中遇到的问题，并及时提出解决问题的建议和操作方法，方式应包括邮件、电话、即时通讯工具等；在服务期内，提供7\*24小时的现场和技术支持服务，对故障15分钟内响应；4小时内到达云机房；

8.2.2 建立全面、及时的监控和预警体系，实现对市文化市场执法总队云资源的统一管理、统计和展示，具备支撑云资源的绩效情况统计能力。能够快速发现和展示网络、主机、存储、应用、虚拟化等资源故障，并能够及时通知相关运维管理人员；

8.2.3 需要保障基础设施资源可扩展性，应具备资源动态调整机制，根据业务系统运行情况进行资源的动态调整；

8.2.4 应为总队建立政务云平台云主机、网络配置策略等信息化技术资料资产档案，为云主机管理和维护提供依据，并于每月月底根据云主机的资源的变更进行档案的更新；

8.2.5 有接受总队政务云平台安全管理相关工作义务，在运维服务期间应按时参加运维监理工作会议，落实监理会议工作要求；

8.2.6 有技术统计与汇报的义务，需每月记录、收集云资源变化情况、云主机杀毒、ATP防护、抗DDOS服务系统安全运行工作情况，并按总队信息化运维工作要求，向总队相关人员汇报工作情况及提交每月运行巡检报告；

8.2.7 应就本项目提出明确的实施方案，并以此作为项目实施过程管理依据；

8.2.8 应按照质量管理和质量保证体系，提出具体措施，确保项目质量。

8.2.9 应充分认识到项目风险管理的重要性，在投标文件中必须分析识别项目中的各类风险因素，并采取相应的对策。

8.2.10提供的运维服务须满足采购人要求，用户满意率达到90%以上，故障响应率达到100%以上，故障排除率达到95%以上，维护响应时间少于30分钟，业务恢复时间少于2小时，并确保全年无重大安全事件。

**（九）备份服务**

**9.1服务内容**

投标人需提供6930GB的租用快照备份服务。

**9.2服务标准**

需利用快照备份云主机设置和磁盘数据，当云主机系统崩溃或软件运行异常时，可以通过快照快速的恢复云主机及磁盘数据。

**（十）日志服务**

**无**

**（十一）迁移服务**

**11.1服务内容**

投标人需提供整体的业务上云迁移服务，应支持X86云主机迁移、X86物理主机迁移、单机数据库迁移、高可用数据库迁移等迁移场景。负责需求调研、架构规划设计、应用迁移部署等工作。

**11.2服务标准**

在本项目服务期内，投标人须承诺不因采购人信息系统在市级政务云平台运行环境发生变化（如现有政务云基础服务供应商资质有效期等客观因素导致的政务云技术环境变化，系统政务云基础服务供应商调整而导致的入云迁移等）而中断提供政务云服务、减少服务内容或降低服务质量；如涉及迁移工作，需提供切实可行的系统迁移方案, 并明确迁移时间，保证现有业务系统在不中断业务的情况下平滑迁移至中标人云平台，确保上述变化所涉及的系统入云迁移、适配等各项工作中，投标人应始终具备必需的技术条件和必要的资源，用以保证采购人信息系统能够始终在市级政务云下保持安全稳定运行，并继续为采购人提供有效的政务云服务，由此产生的全部费用（包括但不限于中标人迁移测试阶段的云资源费用，第三方对业务系统的部署、调试费用等）均由中标人承担。

投标人根据采购人需求完成系统迁移工作，并且不能改变和影响原有系统的功能、技术状态以及采购人的使用习惯。未按时完成系统迁移工作的，采购人有权解除合同并有权要求投标人按合同首付款双倍支付违约金。

**（十二）培训服务**

无

**（十三）其他服务**

根据采购人需求，需提供SSL安全服务（国密）、1项签名验证服务、1项加解密服务、1项时间戳服务。

13.1.1 SSL安全服务（国密）

提供基于SM2/3/4算法的SSL通信信道安全服务，保证用户访问系统以及重要数据传输过程中的机密性和完整性。

13.1.2签名验签服务

为系统提供签名验签、杂凑等密码运算服务，保证重要数据的完整性。

13.1.3加解密服务

实现对称密钥、非对称密钥全生命周期管理，为系统提供数据加解密服务，确保平台中重要数据存储的机密性。

13.1.4时间戳服务

基于国家标准时间源，通过PKI技术为应用系统提供安全、可信的时间戳服务。

1. **运维团队要求**

投标人针对本项目提供专业性强，高效稳定的项目服务保障团队，为本项目扩展服务提供稳定支撑。应分别配备经验丰富的项目经理、技术负责人。

项目经理需具有五年以上类似工作经验，需具备信息系统项目管理师证书（高级）、信息安全保障人员认证证书（安全运维专业级及以上）、具备信息安全保障人员认证证书（应急服务专业级及以上）、具备信创集成项目管理师证书。

技术负责人需具有五年及以上类似项目工作经验，需具备信息安全保障人员认证证书（安全集成专业级及以上）、信息安全保障人员认证证书（应急服务专业级及以上）、注册信息安全工程师（CISE）认证证书。

投标人需设立专业的项目团队，团队在项目经理和技术负责人之外，至少还应配备相关技术人员，并取得有关技术资格认定证书，包括：具有系统规划与管理师资质证书（高级）1人、系统分析师资质证书（高级）1人，系统架构设计师认证证书1人，注册信息安全工程师（CISE）认证1人。

投标人应详细说明实施本项目拟采用的团队组织方法和具体组织机构，保证在此项目实施期间足够的人力投入，并提交与计划相符的项目组人员名单、核心团队相关证书。

1. **商务要求**

**（一）服务地点**

采购人指定

**（二）服务期限**

12个月，从2025年3月10日至2026年3月9日。

**（三）支付方式**

2025年预算批复到账后15个工作日内支付2025年服务期的费用的60%，2025年9月30日前支付2025年服务期的费用的40%，支付第二笔服务费前收取合同总价款10%的履约保函。2026年预算批复到账后15个工作日内支付该合同涉及的2026年服务期的全部服务费用。

**（四）合同要求**

1．采购人与中标人如需变更政府采购合同的相关条款应遵守《中华人民共和国政府采购法》第五章关于政府采购合同的规定。

2．采购人应当加强政务网络和信息系统权限管理，最高管理权限务必由采购人专人负责，按照最小必要原则对投标人进行精细化授权，防范越权访问风险。

**（五）验收服务标准**

1．服务绩效指标

（1）云服务全年整体可用性≥99.9%；

（2）故障响应率100%；

（3）应急响应时间≤5分钟（重大事件1分钟内响应）；

2．项目验收要求

中标人须严格按照服务内容及要求提供服务，应充分满足本招标文件提出的安全保障要求、运维服务要求、迁移服务要求和服务人员要求，制定服务方案并按计划推进执行。

验收时间

中标人于服务合同结束前10个工作日前后，开始筹备运维验收工作，符合验收条件后向采购人提出验收申请。

验收小组

采购人成立验收小组，成员由采购人代表及监理单位组成。

验收方式

采购人组织运维服务验收会议，投标人向采购人汇报运维服务工作情况并提交各项运维数据表单/报告/汇总统计，采购人验收小组成员对上述表单/报告/汇总统计进行验收，查看其数量是否齐全，内容是否完整，验收小组现场出具验收结果，投标人根据验收结果编写《验收报告》，《验收报告》须由采购人、投标人双方盖章确认并各自留存。

1. **保密要求**

（1）投标人因承接本合同约定项目所知悉的该项目信息或采购人信息，以及在项目实施过程中所产生的与该项目有关的全部信息均为采购人的保密信息，投标人应按照采购人关于保密工作的相关要求，对上述保密信息承担保密义务。投标人须严格遵守信息安全规定，不得利用系统维护服务时的便利对采购人数据及其他信息擅自修改或透漏给第三方。

（2）投标人应对上述保密信息予以妥善保存，并保证仅将其用于与完成本合同项下约定项目实施有关的用途或目的。在缺少相关保密条款约定时，对上述保密信息,投标人应至少采取适用于对自己商业秘密进行保护的同等保护措施和审慎程度进行保密。

（3）投标人保证将保密信息的披露范围严格控制在直接从事该项目工作且因工作需要有必要知悉保密信息的工作人员范围内,对投标人非从事该项目的人员一律严格保密。

（4）投标人应保证在向其工作人员披露采购人的保密信息前，认真做好员工的保密教育工作，明确告知其将知悉的为采购人的保密信息，并明确告知其需承担的保密义务及泄密所应承担的法律责任，并要求全体参与该项目的人员签署书面《保密协议》。

（5）任何时间内，一经采购人提出要求，投标人应按照采购人指示在收到采购人书面通知后 5 日内将含有保密信息的所有文件或其他资料归还采购人，且不得擅自复制留存。

（6）非经采购人特别授权，采购人向投标人提供的任何保密信息并不包括授予投标人该保密信息包含的任何专利权、商标权、著作权、商业秘密或其它类型的知识产权。

（7）投标人承担上述保密义务的期限为合同有效期间及合同终止后2年，承担上述保密义务的责任主体为投标人（含投标人服务人员）。

（8）在签订和履行合同过程中从采购人处获知的技术和商业秘密，无论在合同期限内亦或是合同终止后，均应遵守国家有关版权、专利、商标等知识产权方面的法律规定，尊重需求方的知识产权，对所知悉的采购人的技术秘密和商业秘密负有保密责任。

（9）投标人应当对获悉的政务数据、个人信息等予以保密，不得用于其他用途，不得泄露、出售或者非法向他人提供。