**采购需求**

市政府门户网站（“京策”平台）云服务租用

第一包：政策兑现、推演、推送服务系统

政务云服务租用

采购需求

**首都之窗运行管理中心**

**2025年3月**

1. **采购标的**

1. 采购标的

项目名称： 市政府门户网站（“京策”平台）云服务租用

标的名称： 政策兑现、推演、推送服务系统政务云服务租用 ，采购包预算金额

93.764936 万元。

合同履行期限： 自合同签订生效之日起12个月。

本项目是否接受联合体投标：□是 ☑否。

2. 项目概述

为贯彻落实北京市经济和信息化局关于印发《北京市市级政务云管理办法的通知》（京经信委函（2019）150号）文件的要求，我单位现有信息系统“京策”平台的政策兑现系统、政策推演系统、政策推送系统等自2024年起迁入市政务云。现有信息系统情况如下：

2.1政策推演系统

为提升资金扶持性政策的适用性精准度。政策推演系统对具有资金扶持性质的政策，运用大数据智能分析工具，将政策条款与企业用户画像（企业注册地、企业规模、是否上市、企业资质、企业荣誉等标签）进行自动化关联，对拟出台的政策进行兑现结果分析，推演适用企业名单，匡算所需资金总额，预测政策实施效果。系统提供政策条款自动解析、标签数据匹配、资金匡算等功能模块，可自动推演出适用企业名单和分布行业、资金支持额度上限和梯队等次，辅助政策制定部门提高扶持性项目资金预算申请的准确性，增强政策支持企业发展的预见性。

2.2政策审核系统

为提升政策制定的标准性规范性，使政策更加清晰、易懂、实用，建立对政策制定标准性、公开合规性、解读规范性、舆情风险性、兑现操作性、测算必要性等内容的审核程序和机制。政策审核系统提供对政策文件审核的能力，包括政策登记、形式审核、实质审核、批办管理、意见反馈等功能，做到全市政策性文件发布标准统一规范，提高政策的科学性与有效性。政策起草部门在政策登记页面录入政策标题、政策类型等信息并上传政策草稿和解读信息，提交审核，审核人员可对照政策审核要点逐项进行审核，并确认是否符合相应审核要点要求。

2.3政策推送系统

为解决政策“找不到”的问题，“京策”平台政策推送系统探索应用人工智能语义理解和自动拆解能力，解构政策要素，标注政策标签；搭建政策及企业标签体系，将政策条款标签与企业标签建立逻辑关联，匹配出满足政策条款条件的企业名单，并将政策条款推送至相关企业的统一用户空间。企业可登录统一用户空间点击政策服务栏目进行查看，如需申报，企业可点选符合自身条件的政策条款，“一键”进入办事渠道。

2.4政策兑现系统

（1）群众企业申报端

为解决政策兑现渠道散、流程长的问题，“京策”平台在市政府门户网站和“京通”小程序推出“政策兑现专区”，汇聚市区两级涉及财政资金的惠企政策兑现事项，集中全市政策申报入口。专区设置政策匹配、政策清单、项目申报、解读信息、公示公开等功能模块，为群众企业提供惠企政策事项的“一站式”集成、“一键式”申报。

（2）业务部门审批端

政策兑现专区实现了政府各部门审批账号的统一登录，同时可根据不同政策业务需求，定制化搭建初审、复审、专家评审、第三方审核、验收等审批程序，支持多部门跨层级联合在线审批，审批过程全程留痕，提供与企业交互的退回补正，版本对比等功能，缩减兑现周期，同时，针对审批过程中部门对企业申报信息的核验需求，打通各部门之间的数据通道，对企业黑名单、重复申报、虚假申报等进行智能核验、辅助审核，提高审批效率。系统可按实际需求对不同审核岗开放不同审批进度跟踪和查询服务，确保政策兑现的申请与审核流程全面数字化、在线化。

2.5政策事项发布管理

为规范政策兑现事项发布流程，明确政策兑现事项底账，“京策”平台设置政策事项发布管理系统，包括政策管理、事项管理、事项初审、事项复审、统计分析等功能。政策采集人员从各级各部门官网收集到资金扶持性政策后，在系统中录入政策相关信息，由政策事项拆解人员按照申报方向对政策事项进行拆解，由业务部门对申报表单、附件材料、审批环节等内容审核通过后方可进行发布。系统能够实现从搜集、拆解、确认、审核、发布等全流程进行管理，方便业务人员查看政策兑现事项流程状态。

2.6政策服务平台统计分析

为加强对政策落地情况的实时监测分析，“京策”平台设置了北京市政策服务平台数据分析系统，包括政策发布分析、推送情况分析、政策兑现分析、用户反馈分析等功能模块，从政策发布、推送、兑现、反馈4个维度，明确政策发布数、推送企业数、申报企业数、兑付企业数、兑付金额、用户评价反馈等重点评估分析数据，实时掌握全市共出台涉及多少行业领域的政策，分别提供多少资金支持，群众企业对政策的评价情况如何。

1. **商务要求**

1. 交付（实施）的时间（期限）和地点（范围）

服务地点：北京市

服务期限：自合同签订生效之日起12个月。

2. 付款条件（进度和方式）

自合同签署之日，且项目财政资金拨付到位起15个工作日内，支付服务费54286.24元；项目终验后15个工作日内，支付剩余服务费金额。

1. **技术要求**

1. 基本要求

1.1 采购标的需实现的功能或者目标

本项目的总体目标是通过租用政务云平台基础服务，对“京策”平台政策数据、政策问答等相关系统的运行环境进行持续优化，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。

1.2 需执行的国家相关标准、行业标准、地方标准或者其他标准、规范

（1）国家及北京市有关政策

《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）

《国家政务信息化项目建设管理办法》（国办发〔2019〕57号）

《政府采购需求管理办法》(财库〔2021〕22号)

《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）

《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）

《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）

《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）

《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）

《基于云计算的电子政务公共平台顶层设计指南》

《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）

《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）

《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）

《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）

《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）

《北京市政务网络和数据安全管理办法》（京经信发〔2023〕57号）

《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）

（2）国家相关标准

《国家电子政务外网安全接入平台技术规范》

《信息技术—云计算—云服务质量评价指标》（GB/T 37738-2019）

《信息技术—云计算—云服务计量指标》（GB/T 37735-2019）

《信息技术—云计算—云服务采购指南》（GB/T 37734-2019）

《信息技术—云计算—云存储系统服务接口功能》（GB/T 37732-2019）

《信息技术—云计算—云资源监控通用要求》（GB/T 37736-2019）

《信息技术—云计算—云平台间应用和数据迁移指南》（GB/T 37740-2019）

《信息技术—云计算—云服务交付要求》（GB/T 37741-2019）

《信息系统灾难恢复规范》（GB/T 20988-2007）

《信息安全技术 云计算服务安全能力要求》（GB/T 31168-2014）

《信息安全技术网络安全等级保护定级指南》（GB/T22240-2020）

《信息安全技术网络安全等级保护实施指南》（GB/T25058-2019）

《信息安全技术网络安全等级保护安全设计技术要求》（GB/T25070-2019）

《信息安全技术网络安全等级保护基本要求》（GB/T22239-2019）

《信息安全技术网络安全等级保护测评要求》（GB/T28448-20190）

《信息安全技术网络安全等级保护测评过程指南》（GB/T28449-2018）

《信息安全技术网络安全等级保护测试评估技术指南》（GB/T36627-2018）

《信息安全技术 信息系统密码应用基本要求》（GB/T39786-2021）

《信息安全技术 信息安全风险评估方法》（GB/T 20984-2022）

《信息安全技术 云计算服务安全指南》（GB/T 31167-2014）

《信息安全技术 政府网站云计算服务安全指南》（GB/T 38249—2019）

《信息安全技术 云计算安全参考架构》（GB/T 35279—2017）

《信息安全技术 云计算服务安全能力评估方法》GB/T 34942—2017

《信息安全技术 云计算服务运行监管框架》（GB/T 37972—2019）

《信息技术 云资源监控指标体系》（GB/T 37938-2019）

《电子信息系统机房设计规范》（GB50174-2017）

《数据中心电信基础设施标准》（ANSI/TIA-942）

《综合布线系统工程设计规范》（GB 50311—2016）

《云计算关键领域安全指南V4.0》

《信息技术互连国际标准》（ISO/IEC11801-2002）

《信息技术系统间远程通信和信息交换局域网和城域网》GB/T15629.11-2003）

（3）北京市相关标准

《政务云平台建设技术要求》（DB11/T 2169-2023）

《北京市政务云安全技术规范 IaaS云计算平台分册》

《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》

《北京市政务云安全技术规范 信息安全服务接口分册》

（4）其他

《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。**

2. 服务内容及要求

2.1技术要求

（1）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 | 184 | 12 |
| 内存 | 1GB | 元/月 | 488 | 12 |
| 普通性能存储 | 普通存储（单盘技术指标:单盘IOPS1000-3000） | 1GB | 元/月 | 0 | 12 |
| 高性能存储 | 高性能存储（单盘技术指标：单盘IOPS3000-20000） | 1GB | 元/月 | 7400  | 12 |
| 本地备份服务 | 本地备份服务 | 1GB | 元/月 | 1400  | 12 |
| 异地备份服务 | 异地备份服务 | 1GB | 元/月 | 2400  | 12 |
| 互联网链路服务 | 互联网链路带宽 | 1Mb | 元/月 | 20  | 12 |
| 互联网IP地址租用服务、并提供备案服务 | 1IP | 元/月 | 1 | 12 |
| 主机负载均衡服务 | 主机负载均衡服务 | 1IP（内网） | 元/月 | 2  | 12 |
| 远程接入服务 | 远程接入服务 | 1账号 | 元/月 | 3 | 12 |
| WAF防护 | web应用防火墙服务 | 1IP（互联网） | 元/月 | 1 | 12 |
| VPN服务 | SSL VPN接入 | 1套 | 元/月 | 1 | 12 |
| SSL证书服务 | 提供SSL 证书服务，为网站提供https保护，对流量进行加密，防止数据被窃取。 | 1域名 | 元/月 | 1 | 12 |
| 特定云主机深度监控及运维保障服务（7\*24小时值守） | 7\*24小时深度监测云主机资源、硬件设备监控、云平台层应急处置等内容 | 1主机 | 元/月 | 21 | 12 |

（2）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 | 国产Linux套餐：国产Linux操作系统服务租用、安装及维护。 | 1套 | 元/月 | 21 | 12 |
| 国产商用应用中间件套餐 | 国产商用应用中间件租用、安装及维护 | 1套 | 元/月 | 4 | 12 |
| 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 | 4 | 12 |
| 安全服务 | 云端抗DDOS服务 | 云端抗DDOS服务 | 1 站点 | 元/月 | 1 | 12 |
| 云端APT防护服务 | 云端APT防护服务 | 1 套 | 元/月 | 1 | 12 |
| 主机杀毒服务 | 主机杀毒服务 | 1台 | 元/月 | 21  | 12 |
| 主机防护 | 主机防护 | 1月 | 元/月 | 21  | 12 |
| 主机安全加固 | 主机安全加固 | 1台 | 元/次 | 84 | 12 |
| 网页防篡改服务 | 网页防篡改服务 | 1月 | 元/月 | 1  | 12 |
| 安全检测监测、审计服务 | 主机漏洞扫描 | 主机漏洞扫描 | 1次 | 元/次 | 84 | 12 |
| 主机日志审计服务 | 主机日志审计服务 | 1次 | 元/月 | 21 | 12 |
| 数据库审计服务 | 数据库审计服务 | 1次 | 元/月 | 4 | 12 |
| 其他服务 | 密码应用安全支撑服务 | 提供身份认证、数据加解密、数据安全传输 、签名验签、密钥管理等密码应用安全支撑服务 | 1月 | 元/月 | 1 | 12 |

2.2服务内容及标准

2.2.1云主机服务

2.2.1.1服务内容

按照采购人的具体需求，提供云主机服务，可按需求对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。

2.2.1.2服务标准

（1）云主机应实现物理机的全部功能，如具有CPU、存储、内存、网卡等资源，可以指定单独的IP地址、MAC地址等；

（2）支持存储裸设备映射（RDM），可以将存储设备上的LUN直接映射给虚拟机使用，并且支持SCSI指令使用透传模式或者非透传模式；

（3）应满足云主机之间、CPU之间隔离保护要求；

（4）支持资源的动态调整，根据业务的负载情况实现业务系统虚拟机的动态扩展和回收，支持手动和自动方式，自动方式可基于主机的CPU、内存、磁盘IO、网络流量等性能参数阈值进行动态调度；

（5）支持在线进行虚拟化软件版本升级，不同版本之间可以相互兼容；

（6）支持异构虚拟化能力，如KVM、PowerVM等多种虚拟化技术；

（7）云主机出现故障时，支持自动重启或者迁移，保障业务连续性；

（8）支持虚拟机热迁移，可在不同代CPU资源池中进行虚拟机热迁移；

（9）云计算资源性能要求包括但不限于如下：

* 物理服务器CPU主频应不低于2.4GHz；
* 可用性不低于99.99%。

2.2.2存储服务

2.2.2.1服务内容

按照采购人的具体需求，提供存储服务，包括：普通性能存储、高性能存储、本地备份和异地备份服务服务，实现合理的存储资源配置。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。

2.2.2.2服务标准

（1）支持结构化数据、半结构化数据和非结构化数据等多种数据类型存储；

（2）支持块存储、对象存储、文件存储等多种存储方法，满足数据备份、视频存储等不同应用场景使用要求；

（3）支持存储资源扩展能力，例如：PB级扩展；

（4）支持磁盘容错技术，如磁盘故障后节点的自动平衡和重构、硬盘故障检测和处理、集群节点出现单盘故障时不影响业务运行等；

（5）存储资源性能要求包括但不限于如下：

* 支持高可靠性，可靠性不低于99.9999%；
* 对于块存储服务，支持普通性能、高性能两类，普通存储单盘技术指标：IOPS大于等于2000，高性能存储单盘技术指标：IOPS大于等于10000。

2.2.3数据库服务

2.2.3.1服务内容

（1）数据库租用服务

按照采购人的有关管理规定及具体需求，提供数据库租用服务。

（2）数据库安全加固服务

按照采购人的有关管理规定及具体需求，提供针对预警自查、漏洞扫描或等级测评结果对数据库进行安全加固及升级，用以解决等级测评结果中所显示的漏洞。

（3）数据库运维

对数据库操作行为进行细粒度审计的合规性管理，对数据库遭受到的风险行为进行告警，对攻击行为进行阻断。对用户访问数据库行为的记录、分析和汇报，生成合规报告以及事故追根溯源。

2.2.3.2服务标准

（1）支持主流国产软硬件体系，支持飞腾系列、鲲鹏系列、海光系列等不同 CPU架构；支持麒麟、统信UOS等多种主流国产操作系统；

（2）支持全文检索、支持设置权重，支持相关性排序功能；

（3）产品具备完全自主知识产权，避免潜在的版权纠纷；

（4）支持集中式运维管理工具，支持集群监控、告警等功能。

2.2.4网络服务

2.2.4.1服务内容

（1）提供互联网链路带宽服务、互联网IP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。

（2）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。

（3）远程接入服务，提供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）VPN服务，含SSL VPN接入服务。

2.2.4.2服务标准

网络系统提供稳定的数据传输能力，一般要求如下：

（1）具备多运营商网络接入服务的能力；

（2）数据中心组网架构设计可采用大二层网络架构，支持云主机无障碍动态迁移；

（3）应采用集群部署网络控制，以保障升级时业务不中断；

（4）应实现自动化动态网络资源调配和隔离，支持与互联网、电子政务外网及行业部门专网的连接；

（5）支持IPv6地址分配，满足业务系统IPv6要求；

（6）具备边界防火墙和VPC防火墙隔离能力，分别针对不同的流量进行安全策略防护与配置；

（7）具备高可用虚拟IP能力，在集群或主备场景下，云主机可绑定高可用虚拟IP，达到高可用访问效果；

（8）采用双活网络架构，降低单点故障带来的稳定风险；为入云系统划分安全区域，合理制定访问规则。

（9）网络系统性能要求包括但不限于如下：

* 云内骨干线路带宽不低于20Gb/s；
* 服务器业务带宽不低于10Gb/s；
* 平均可用性不低于99.99%。

（10）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；

（11）SSL VPN接入须实现Web接入，TCP接入，IP接入等多种方式，能够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。

（12）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。

2.2.5基础软件支撑服务

2.2.5.1服务内容

按照采购人的有关管理规定及具体需求，提供国产商用操作系统、国产商用应用中间件、国产商用数据库、等软件支撑服务。

2.2.5.2服务标准

（1）国产商用操作系统套餐

提供主流商业操作系统服务，支持国产Linux操作系统（银河麒麟/中标麒麟/统信等）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。

（2）国产商用应用中间件套餐

提供主流国产商用中间件服务，支持金蝶、东方通、普元等3种以上国产中间件的主流版本，并提供中间件的安装部署以及各种故障处理和日常维护。

（3）国产商用数据库套餐

提供主流国产商用数据库服务，支持3种及以上国产数据库单机、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。

2.2.6资源调度服务

2.2.6.1服务内容

（1）提供以云主机为核心的容器管理服务，为云主机提供高效部署、资源调度等一系列完整功能：

* 具备资源管理能力；
* 具备多集群管理能力；
* 具备多租户管理能力；
* 具备运维系统、监控系统等基本功能；
* 具备自动清理闲置容器镜像能力，并可自定义最大保留时长；
* 通过升级检查后，支持自动化低版本容器管理平台向高版本升级，通过升级检查后，可进行全自动化。

（2）弹性伸缩

* 提供以云主机为核心的动态伸缩功能；
* 提供资源分配与调度功能，包括统计资源利用率，并能够按照策略动态分配资源；
* 提供动态迁移功能，包括伸缩迁移、故障迁移等功能；

2.2.6.2服务标准

按照采购人的具体需求，提供资源调度服务，投标人应具备以下能力：

（1）投标人应对自身云资源池容量进行管理，对资源总量（计算、存储、带宽）及已分配资源、未分配资源进行监控，当平台某资源的已分配量超过该资源总量80%时，须承诺实现7个自然日快速扩容。

（2）投标人需要保障基础设施资源可扩展性，满足所有用户需求，能够在多租户网络流量条件下，对用户网络流量进行识别并进行精细化管理。

（3）投标人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，并承诺短期内提供云资源扩展服务（不超过原有资源的20%）。

（4）投标人应按内存不复用方式分配云资源。

2.2.7安全服务

2.2.7.1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。安全服务主要内容包含：

（1）WAF防护服务

按照采购人的具体需求，提供互联网WAF防护服务，保证用户对已知安全隐患进行防护，实时升级漏洞补丁，配置防护策略，起到前端防护作用。

（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。

（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。

（4）主机杀毒服务

提供主机杀毒服务，对云主机进行定期的病毒查杀，实施杀毒软件集中控制。

（5）主机安全加固

提供主机安全加固服务，针对预警自查、漏洞扫描或等级测评结果对操作系统进行安全加固，用以解决等级测评结果中所显示的漏洞。

（6）网页防篡改服务

按照采购人的具体需求，提供网页防篡改服务。通过防篡改软件对用户页面进行实时防护，减少用户页面被恶意篡改的可能性。

（7）主机防护服务

提供符合等保三级要求的主机权限管理及安全防护。可对主机系统安全涉及的控制点形成立体防护。

（8）主机漏洞扫描

基于漏洞数据库，通过扫描等手段对主机安全脆弱性进行检测。

2.2.7.2服务标准

（1）投标人所投云平台具备完备的安全防护体系和安全防护设备，具有成熟的安全运维方案，应保证各业务应用系统的支撑环境，包括但不限于服务器、网络、存储以及相关物理环境，应能满足不低于网络安全等级保护（GB/T22239-2019）第三级要求，并积极配合采购人根据各业务系统具体等保需求，开展相应等保评估、检查、整改等工作。

（2）投标人需利用监控系统或人工硬件设备及应用系统的运行情况进行7\*24小时的不间断巡检监控，及时发现安全隐患，通知相关人员及时处理，并形成监控报告。每周反馈日志审计和数据库审计报告，进行总结分析。

（3）投标人需纳入行业监管部门网络安全保障整体工作体系，在涉及重保、安全事件、威胁情报等方面，配合安全服务商开展研判、处置、分析等工作。

（4）投标人承担云平台数据防篡改、防丢失的安全责任。业务数据未经采购人同意，不得离开云机房。投标人未经允许不得对云平台上的任何数据进行非法截取、加工、分析处理或提供给第三方机构。投标人在未经过用户邮件、书面材料确认前提下，不能查看、修改、拷贝用户业务系统文件和数据；各业务系统、数据归属于采购人，投标人无权支配。

（5）投标人需保证安全技术服务能力不低于所承载的信息系统的最高级别，并通过GB/T 22239相应等级的测评；符合GB/T 34080.1，GB/T 34080.2，GB/T 34080.3，GB/T 34080.4中的规定；通过商用密码应用安全性评估，商用密码应用安全性评估参考GB/T 39786-2021中相应等级规定；保障其上的租户安全、云主机安全、业务安全和数据安全；

（6）投标人应坚持制度和技术并重，建立健全网络和数据安全管理制度，落实网络和数据安全管理要求。采取相应技术措施，保障网络免受干扰、破坏或者未经授权的访问，防止数据泄露或者被窃取、篡改、破坏。

（7）对于关键信息基础设施，应当落实网络安全审查要求，采购网络产品和服务的，应当预判该产品和服务投入使用后可能带来的国家安全风险，确保采购国产化的网络产品和服务。影响或者可能影响国家安全的，应当申报网络安全审查。

（8）定期开展数据安全风险评估，发现数据安全隐患风险时，应当及时整改加固，采取必要的安全保护措施，防范数据安全风险。

（9）投标人应明确接触网络和信息系统、数据时的申请及审批流程，做好实名登记、权限控制、保密协议签署等管理。

（10）在服务期内，承载政务云平台的软硬件应在原厂维保期限内。

2.2.8运维服务

2.2.8.1服务内容

（1）负责云平台硬件资产、虚拟化资产的管理工作；

（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；

（3）执行云平台变更申请、审批流程；

（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；

（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。

2.2.8.2服务标准

（1）依据《北京市市级政务云管理办法》，投标人应当提供高效的系统维护服务，有效防范系统风险，系统对应负责人7\*24小时电话畅通，能够在系统发生除宕机外的其他故障问题时，能够协调人力资源在1小时内到达政务云机房现场提供服务。系统发生宕机问题时，投标人应在5分钟内响应，能够协调人力资源在1小时内到达运维现场定位、排除故障，在4个小时之内使系统恢复正常，故障处理完毕后提供相关系统宕机报告。

（2）为保障业务高峰期内系统平稳运行，缓解系统高峰期内因业务发生量增大而带来系统压力风险，要求投标人根据业务周期性特点，加大运维保障力度，保证在业务高峰期内系统平稳运行。

（3）重点保障时期重要信息系统云主机资源调整时间不超过4小时，针对重点保障时期的重要信息系统重要云主机，投标人应按采购人要求进行实时监控，超过预警阈值时主动上调云资源，并第一时间通知采购人进行相应操作，确保系统平稳运行。

（4）按照国家、北京市相关规定和信息安全技术标准及规范要求, 落实安全保障措施, 通过信息安全测评机构的测评和政务云安全审查 。

（5）投标人应明确运维操作规范和工作流程。定期开展文档查阅、漏洞扫描、渗透测试等多种形式的安全自查，排查政务网络和信息系统可能存在的安全漏洞，以及木马、后门、病毒等隐患风险，及时进行整改加固，切实防范安全风险。

（6）投标人应建立政务网络和数据安全监测通报机制，加强网络和数据安全监测，及时发布预警信息，开展政务网络和数据安全应急保障工作。发现其网络产品或服务存在安全漏洞等隐患风险时，应当立即采取补救措施，按照规定及时告知采购人并向有关监管部门报告。

（7）投标人应保障政务云规范运行。入云系统应开展网络安全测评及备案。应对数据进行分类分级管理，根据数据分级保护要求采取相应级别的安全防护措施；应按相关要求对重要数据进行异地备份。

（8）除不可抗力或计划内维护作业造成的政务云服务中断外,政务云实行24小时不间断运行。

2.2.9备份服务

2.2.9.1服务内容

投标人需具有本地和同城异地数据级备份能力，并配合采购人完成数据级容灾演练及恢复等工作。

2.2.9.2服务标准

按照采购人的各个应用系统对资源的备份需求通过备份策略实现对用户数据（文件、操作系统、数据库）的本地备份/异地备份（不包含备份存储空间费用），默认提供非结构化数据保护与文件备份保护。备份应满足如下要求:

（1）备份介质本身具备高可用性和冗余性。

（2）备份方式包括完整备份、差异备份和增量备份。

（3）支持Windows系列操作系统、Linux主流系统操作系统、主流数据库软件、主流中间件软件、结构化数据以及非结构化数据等备份对象。

（4）支持建立统一的备份管理系统，用来管理本地备份和异地备份。

（5）投标人应提供对备份过程状态、备份结果提供运维监控保障服务，确保备份任务执行成功以及备份的数据完整性。

2.2.10日志服务

2.2.10.1服务内容

日志是发现问题、定位问题的重要信息，投标人提供统一的日志平台服务，针对操作系统进行日志收集，用于了解主机安全情况及资源使用情况，具体内容如下：

（1）支持的日志格式包括Web Service、Syslog、SNMP、JDBC、ODBC、HTTP/FTP、JASON等多种类型；

（2）支持通过统一的日志采集设备，对市级政务云内各类主机进行日志收集，并进行进一步的分析计算；

（3）支持结合威胁情报针对主机日志采集的高级威胁攻击进行检测；

（4）通过对主机日志数据分析，实现对用户和业务访问的精细化管理，建立网络流量的多种流量基线，从而为后续的链路、带宽和服务器扩容提供技术支撑；

（5）支持自定义日志副本数；

2.2.10.2服务标准

对主机系统日志进行采集分析处理，用于发现各种安全威胁、异常行为事件。主机系统日志应集中存储，且日志存储时间不低于6个月。

2.2.11迁移服务

2.2.11.1服务内容

如需迁移，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、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、配合架构规划设计、配合应用迁移部署等工作。

2.2.11.2服务标准

本项目涉及的业务系统为采购人在用的生产系统，目前在政务云上平稳运行，因此保障业务连续性是重要的保障需求。迁移服务具体要求如下：

（1）投标人需编制业务连续性服务方案。

（2）本项目如涉及系统迁移，在连续性服务方案中需提供确实可行的迁移部署服务子方案，迁移部署服务子方案应包括（但不限于）迁移部署流程（包含但不限于应用、虚拟机和数据类迁移）、业务系统部署迁移方案。迁移部署服务子方案应明确需要采购人配合的具体工作内容及时长，针对系统迁移过程中容易造成业务系统中断的环节，包含但不限于互联网及政务外网IP变更割接、业务数据同步及切换上线、应急回退方案等，进行风险评估，提出详细解决方案。

（3）本项目如涉及系统迁移，为保障业务系统的连续性，投标人应承诺自中标之日起，积极与原服务商对接，在20个工作日内，完成系统迁移平滑过渡，且因此产生的各项费用（包括但不限于测试阶段的云资源费用，系统开发商对业务系统的部署、调试费用等），应包含在投标人的报价中，提供“承诺函”并加盖投标人公章。

2.2.12其他服务

按照采购人的有关管理规定及具体需求提供个性化服务，包括密码应用安全支撑服务。

按照采购人有关国产密码应用改造等相关需求，提供咨询、评估、论证、使用等支撑保障服务，密码服务包括提供SSL证书、身份认证、数据加解密、数据安全传输 、签名验签、密钥管理等密码应用安全支撑服务。

2.3运维团队要求

（1）服务期内，投标人须设有7×24小时电话响应服务、具备运维团队，提供售后服务保障。团队成员应明确职责，架构清晰，岗位设置合理，且具备与本项目相关的项目经验。

（2）投标人须提供1名项目经理、1名安全技术负责人及2名项目团队专职人员，为本项目提供服务。项目经理及安全负责人需按照采购人要求，承担云资源服务保障具体工作，技术支持人员要求如下：

**服务团队人员要求**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 岗位 | 数量 | 学历 | 工作经验 | 岗位需具备的上岗资格证等要求 |
| 项目经理 | 1 | 本科及以上 | 有5年及以上类似工作经验 | 1、信息系统项目管理师2、信息安全保障人员认证证书（安全运维专业级或专业高级）3、信息安全保障人员认证证书（应急服务专业级或以上） |
| 安全技术负责人 | 1 | 本科及以上 | 有5年及以上类似工作经验 | 1、信息安全保障人员认证证书（安全集成专业级或以上）2、信息安全保障人员认证证书（应急服务专业级或以上）3、注册信息安全工程师证书（CISP） |
| 项目人员 | 2 | 本科及以上 | 有5年及以上类似工作经验 | 1、系统规划与管理师资质证书（高级）2、系统分析师资质证书（高级）3、系统架构设计师认证证书（高级）4、注册信息安全工程师证书（CISP） |

3. 验收标准

3.1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）。

3.2项目验收要求

（1）投标人所提供的北京市市级政务云基础资源服务应遵循客观、科学、合理的原则，符合《北京市市级政务云管理办法》的相关标准及要求。

（2）投标人所提供资源应满足采购文件规定的要求。保证合同期内系统安全稳定运行，不因硬件故障导致服务中断4小时及以上。

（3）服务期满后10个工作日开始对合同项目进行验收，投标人应当在采购人指定的验收日前向采购人提交验收报告。验收报告的内容包括但不限于，合同规定的各项服务清单，各系统设备运行情况。

（4）服务期届满，投标人按照采购人要求完成所有项目，各项记录、报告等文档齐全，无任何系统遗留问题，并通过由采购人组织的专家验收评审，方可通过验收。

4. 其他要求（如有）

4.1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）对于分包事项（如等保测评、密码应用安全性评估等），采购人应当对分包承接主体的网络安全能力进行评估，与网络服务提供者签订合同及保密协议，明确约定各方保障网络和数据安全的权利及义务。投标人应当具备网络和数据安全管理能力及相关资质，对提供产品和服务的安全性、合规性负责。发生网络安全事件时，在依法按程序报告的同时，投标人应当及时向采购人报告，并有义务配合调查。

（3）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。

4.2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。

4.3知识产权要求

（1）投标人应确保本项目所提交成果无知识产权纠纷，项目成果的知识产权属于项目委托方。须在响应文件中对此项作出专项承诺，格式自拟。

（2）投标人保证向采购人提供的服务成果是其独立实施完成，不存在任何侵犯第三方专利权、商标权、著作权等合法权益。如因投标人提供的服务成果侵犯任何第三方的合法权益，导致该第三方追究采购人责任的，投标人应负责解决并赔偿因此给采购人造成的全部损失。

市政府门户网站（“京策”平台）云服务租用

第二包：政策数据、问答服务系统政务云服务租用

采购需求

**首都之窗运行管理中心**

**2025年3月**

1. **采购标的**

1. 采购标的（货物需求一览表或简要服务内容及数量）

项目名称： 市政府门户网站（“京策”平台）云服务租用

标的名称： 政策数据、问答服务系统政务云服务租用 ，采购包预算金额

162.374092 万元。

合同履行期限： 自合同签订生效之日起12个月。

本项目是否接受联合体投标：□是 ☑否。

2. 项目概述

为贯彻落实北京市经济和信息化局关于印发《北京市市级政务云管理办法的通知》（京经信委函（2019）150号）文件的要求，我单位现有信息系统“京策”平台的政策数据系统、问答服务系统自2024年起迁入市政务云。现有信息系统情况如下：

（1）政策数据运维系统

提供我单位工作的全流程支撑能力，包括优化搜索功能、政策解构功能、政策库（文件库、条款库、解读库、事项库）存储功能、政策标签管理及自动标注功能，以及各类资料、文件查阅的能力。

（2）问答服务系统

主要服务对象为互联网用户，相关部门通过该系统实现智能解答功能，提供政策知识检索、政策知识推荐、政策知识问答、智能办事等功能；根据用户提交问题智能匹配所需政策信息。

1. **商务要求**

1. 交付（实施）的时间（期限）和地点（范围）

服务地点：北京市

服务期限：自合同签订生效之日起12个月。

2. 付款条件（进度和方式）

自合同签署之日，且项目财政资金拨付到位起15个工作日内，支付服务费94008.27元；项目终验后15个工作日内，支付剩余服务费金额。

1. **技术要求**

1. 基本要求

1.1 采购标的需实现的功能或者目标

本项目的总体目标是通过租用政务云平台基础服务，对“京策”平台政策数据、政策问答等相关系统的运行环境进行持续优化，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。

1.2 需执行的国家相关标准、行业标准、地方标准或者其他标准、规范

（1）国家及北京市有关政策

《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）

《国家政务信息化项目建设管理办法》（国办发〔2019〕57号）

《政府采购需求管理办法》(财库〔2021〕22号)

《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）

《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）

《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）

《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）

《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）

《基于云计算的电子政务公共平台顶层设计指南》

《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）

《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）

《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）

《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）

《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）

《北京市政务网络和数据安全管理办法》（京经信发〔2023〕57号）

《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）

（2）国家相关标准

《国家电子政务外网安全接入平台技术规范》

《信息技术—云计算—云服务质量评价指标》（GB/T 37738-2019）

《信息技术—云计算—云服务计量指标》（GB/T 37735-2019）

《信息技术—云计算—云服务采购指南》（GB/T 37734-2019）

《信息技术—云计算—云存储系统服务接口功能》（GB/T 37732-2019）

《信息技术—云计算—云资源监控通用要求》（GB/T 37736-2019）

《信息技术—云计算—云平台间应用和数据迁移指南》（GB/T 37740-2019）

《信息技术—云计算—云服务交付要求》（GB/T 37741-2019）

《信息系统灾难恢复规范》（GB/T 20988-2007）

《信息安全技术 云计算服务安全能力要求》（GB/T 31168-2014）

《信息安全技术网络安全等级保护定级指南》（GB/T22240-2020）

《信息安全技术网络安全等级保护实施指南》（GB/T25058-2019）

《信息安全技术网络安全等级保护安全设计技术要求》（GB/T25070-2019）

《信息安全技术网络安全等级保护基本要求》（GB/T22239-2019）

《信息安全技术网络安全等级保护测评要求》（GB/T28448-20190）

《信息安全技术网络安全等级保护测评过程指南》（GB/T28449-2018）

《信息安全技术网络安全等级保护测试评估技术指南》（GB/T36627-2018）

《信息安全技术 信息系统密码应用基本要求》（GB/T39786-2021）

《信息安全技术 信息安全风险评估方法》（GB/T 20984-2022）

《信息安全技术 云计算服务安全指南》（GB/T 31167-2014）

《信息安全技术 政府网站云计算服务安全指南》（GB/T 38249—2019）

《信息安全技术 云计算安全参考架构》（GB/T 35279—2017）

《信息安全技术 云计算服务安全能力评估方法》GB/T 34942—2017

《信息安全技术 云计算服务运行监管框架》（GB/T 37972—2019）

《信息技术 云资源监控指标体系》（GB/T 37938-2019）

《电子信息系统机房设计规范》（GB50174-2017）

《数据中心电信基础设施标准》（ANSI/TIA-942）

《综合布线系统工程设计规范》（GB 50311—2016）

《云计算关键领域安全指南V4.0》

《信息技术互连国际标准》（ISO/IEC11801-2002）

《信息技术系统间远程通信和信息交换局域网和城域网》GB/T15629.11-2003）

（3）北京市相关标准

《政务云平台建设技术要求》（DB11/T 2169-2023）

《北京市政务云安全技术规范 IaaS云计算平台分册》

《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》

《北京市政务云安全技术规范 信息安全服务接口分册》

（4）其他

《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。**

2. 服务内容及要求

2.1技术要求

（1）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 | 340  | 12 |
| 内存 | 1GB | 元/月 | 832  | 12 |
| 普通性能存储 | 普通存储（单盘技术指标:单盘IOPS1000-5000） | 1GB | 元/月 | 4900  | 12 |
| 高性能存储 | 高性能存储（单盘技术指标：单盘IOPS10000-25000） | 1GB | 元/月 | 8500  | 12 |
| 本地备份服务 | 本地备份服务 | 1GB | 元/月 | 1000  | 12 |
| 异地备份服务 | 异地备份服务 | 1GB | 元/月 | 1000  | 12 |
| 互联网链路服务 | 互联网链路带宽 | 1Mb | 元/月 | 80  | 12 |
| 互联网IP地址租用服务、并提供备案服务 | 1IP | 元/月 | 4  | 12 |
| 主机负载均衡服务 | 主机负载均衡服务 | 1IP（内网） | 元/月 | 10  | 12 |
| 远程接入服务 | 远程接入服务 | 1账号 | 元/月 | 2  | 12 |
| WAF防护 | web应用防火墙服务 | 1IP（互联网） | 元/月 | 2 | 12 |
| VPN服务 | SSL VPN接入 | 1套 | 元/月 | 10 | 12 |
| 特定云主机深度监控及运维保障服务（7\*24小时值守） | 7\*24小时深度监测云主机资源、硬件设备监控、云平台层应急处置等内容 | 1主机 | 元/月 | 29 | 12 |

（2）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 | 国产Linux套餐：国产Linux操作系统服务租用、安装及维护。 | 1套 | 元/月 | 29 | 12 |
| 国产商用应用中间件套餐 | 国产商用应用中间件租用、安装及维护 | 1套 | 元/月 | 14 | 12 |
| 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 | 6  | 12 |
| 安全服务 | 云端抗DDOS服务 | 云端抗DDOS服务 | 1 站点 | 元/月 | 4  | 12 |
| 云端APT防护服务 | 云端APT防护服务 | 1 套 | 元/月 | 4  | 12 |
| 主机杀毒服务 | 主机杀毒服务 | 1台 | 元/月 | 29  | 12 |
| 主机防护 | 主机防护 | 1月 | 元/月 | 29  | 12 |
| 主机安全加固 | 主机安全加固 | 1台 | 元/次 | 116  | 12 |
| 安全检测监测、审计服务 | 主机漏洞扫描 | 主机漏洞扫描 | 1次 | 元/次 | 116 | 12 |
| 主机日志审计服务 | 主机日志审计服务 | 1次 | 元/次 | 29 | 12 |
| 数据库审计服务 | 数据库审计服务 | 1次 | 套 | 2 | 12 |
| 其他服务 | 密码应用安全支撑服务 | 提供SSL证书、身份认证、数据加解密、数据安全传输 、签名验签、密钥管理等密码应用安全支撑服务 | 1月 | 元/月 | 1 | 12 |

2.2服务内容及标准

2.2.1云主机服务

2.2.1.1服务内容

按照采购人的具体需求，提供云主机服务，可按需求对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。

2.2.1.2服务标准

（1） 云主机应实现物理机的全部功能，如具有CPU、存储、内存、网卡等资源，可以指定单独的IP地址、MAC地址等；

（2）支持存储裸设备映射（RDM），可以将存储设备上的LUN直接映射给虚拟机使用，并且支持SCSI指令使用透传模式或者非透传模式；

（3）应满足云主机之间、CPU之间隔离保护要求；

（4）支持资源的动态调整，根据业务的负载情况实现业务系统虚拟机的动态扩展和回收，支持手动和自动方式，自动方式可基于主机的CPU、内存、磁盘IO、网络流量等性能参数阈值进行动态调度；

（5）支持在线进行虚拟化软件版本升级，不同版本之间可以相互兼容；

（6）支持异构虚拟化能力，如KVM、PowerVM等多种虚拟化技术；

（7）云主机出现故障时，支持自动重启或者迁移，保障业务连续性；

（8）支持虚拟机热迁移，可在不同代CPU资源池中进行虚拟机热迁移；

（9）云计算资源性能要求包括但不限于如下：

* 物理服务器CPU主频应不低于2.4GHz；
* 可用性不低于99.99%。

2.2.2存储服务

2.2.2.1服务内容

按照采购人的具体需求，提供存储服务，包括：普通性能存储、高性能存储、本地备份和异地备份服务服务，实现合理的存储资源配置。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。

2.2.2.2服务标准

（1）支持结构化数据、半结构化数据和非结构化数据等多种数据类型存储；

（2）支持块存储、对象存储、文件存储等多种存储方法，满足数据备份、视频存储等不同应用场景使用要求；

（3）支持存储资源扩展能力，例如：PB级扩展；

（4）支持磁盘容错技术，如磁盘故障后节点的自动平衡和重构、硬盘故障检测和处理、集群节点出现单盘故障时不影响业务运行等；

（5）存储资源性能要求包括但不限于如下：

* 支持高可靠性，可靠性不低于99.9999%；
* 对于块存储服务，支持普通性能、高性能两类，普通存储单盘技术指标：IOPS大于等于2000，高性能存储单盘技术指标：IOPS大于等于10000。

2.2.3数据库服务

2.2.3.1服务内容

（1）数据库租用服务

按照采购人的有关管理规定及具体需求，提供数据库租用服务。

（2）数据库安全加固服务

按照采购人的有关管理规定及具体需求，提供针对预警自查、漏洞扫描或等级测评结果对数据库进行安全加固及升级，用以解决等级测评结果中所显示的漏洞。

（3）数据库运维

对数据库操作行为进行细粒度审计的合规性管理，对数据库遭受到的风险行为进行告警，对攻击行为进行阻断。对用户访问数据库行为的记录、分析和汇报，生成合规报告以及事故追根溯源。

2.2.3.2服务标准

（1）支持主流国产软硬件体系，支持飞腾系列、鲲鹏系列、海光系列等不同 CPU架构；支持麒麟、统信UOS等多种主流国产操作系统；

（2）支持全文检索、支持设置权重，支持相关性排序功能；

（3）产品具备完全自主知识产权，避免潜在的版权纠纷；

（4）支持集中式运维管理工具，支持集群监控、告警等功能。

2.2.4网络服务

2.2.4.1服务内容

（1）提供互联网链路带宽服务、互联网IP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。

（2）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。

（3）远程接入服务，提供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）VPN服务，含SSL VPN接入服务。

2.2.4.2服务标准

网络系统提供稳定的数据传输能力，一般要求如下：

（1）具备多运营商网络接入服务的能力；

（2）数据中心组网架构设计可采用大二层网络架构，支持云主机无障碍动态迁移；

（3）应采用集群部署网络控制，以保障升级时业务不中断；

（4）应实现自动化动态网络资源调配和隔离，支持与互联网、电子政务外网及行业部门专网的连接；

（5）支持IPv6地址分配，满足业务系统IPv6要求；

（6）具备边界防火墙和VPC防火墙隔离能力，分别针对不同的流量进行安全策略防护与配置；

（7）具备高可用虚拟IP能力，在集群或主备场景下，云主机可绑定高可用虚拟IP，达到高可用访问效果；

（8）采用双活网络架构，降低单点故障带来的稳定风险；为入云系统划分安全区域，合理制定访问规则。

（9）网络系统性能要求包括但不限于如下：

* 云内骨干线路带宽不低于40Gb/s；
* 服务器业务带宽不低于10Gb/s；
* 平均可用性不低于99.99%。

（10）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；

（11）SSL VPN接入须实现Web接入，TCP接入，IP接入等多种方式，能够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。

（12）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。

2.2.5基础软件支撑服务

2.2.5.1服务内容

按照采购人的有关管理规定及具体需求，提供国产商用操作系统、国产商用应用中间件、国产商用数据库、等软件支撑服务。

2.2.5.2服务标准

（1）国产商用操作系统套餐

提供主流商业操作系统服务，支持国产Linux操作系统（银河麒麟/中标麒麟/统信等）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。

（2）国产商用应用中间件套餐

提供主流国产商用中间件服务，支持金蝶、东方通、普元等3种以上国产中间件的主流版本，并提供中间件的安装部署以及各种故障处理和日常维护。

（3）国产商用数据库套餐

提供主流国产商用数据库服务，支持3种及以上国产数据库单机、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。

2.2.6资源调度服务

2.2.6.1服务内容

（1）提供以云主机为核心的容器管理服务，为云主机提供高效部署、资源调度等一系列完整功能：

* 具备资源管理能力；
* 具备多集群管理能力；
* 具备多租户管理能力；
* 具备运维系统、监控系统等基本功能；
* 具备自动清理闲置容器镜像能力，并可自定义最大保留时长；
* 通过升级检查后，支持自动化低版本容器管理平台向高版本升级，通过升级检查后，可进行全自动化。

（2）弹性伸缩

* 提供以云主机为核心的动态伸缩功能；
* 提供资源分配与调度功能，包括统计资源利用率，并能够按照策略动态分配资源；
* 提供动态迁移功能，包括伸缩迁移、故障迁移等功能；

2.2.6.2服务标准

按照采购人的具体需求，提供资源调度服务，投标人应具备以下能力：

（1）投标人应对自身云资源池容量进行管理，对资源总量（计算、存储、带宽）及已分配资源、未分配资源进行监控，当平台某资源的已分配量超过该资源总量80%时，须承诺实现7个自然日快速扩容。

（2）投标人需要保障基础设施资源可扩展性，满足所有用户需求，能够在多租户网络流量条件下，对用户网络流量进行识别并进行精细化管理。

（3）投标人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，并承诺短期内提供云资源扩展服务（不超过原有资源的20%）。

（4）投标人应按内存不复用方式分配云资源。

2.2.7安全服务

2.2.7.1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。安全服务主要内容包含：

（1）WAF防护服务

按照采购人的具体需求，提供互联网WAF防护服务，保证用户对已知安全隐患进行防护，实时升级漏洞补丁，配置防护策略，起到前端防护作用。

（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。

（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。

（4）主机杀毒服务

提供主机杀毒服务，对云主机进行定期的病毒查杀，实施杀毒软件集中控制。

（5）主机安全加固

提供主机安全加固服务，针对预警自查、漏洞扫描或等级测评结果对操作系统进行安全加固，用以解决等级测评结果中所显示的漏洞。

（6）主机防护服务

提供符合等保三级要求的主机权限管理及安全防护。可对主机系统安全涉及的控制点形成立体防护。

（7）主机漏洞扫描

基于漏洞数据库，通过扫描等手段对主机安全脆弱性进行检测。

2.2.7.2服务标准

（1）投标人所投云平台具备完备的安全防护体系和安全防护设备，具有成熟的安全运维方案，应保证各业务应用系统的支撑环境，包括但不限于服务器、网络、存储以及相关物理环境，应能满足不低于网络安全等级保护（GB/T22239-2019）第三级要求，并积极配合采购人根据各业务系统具体等保需求，开展相应等保评估、检查、整改等工作。

（2）投标人需利用监控系统或人工硬件设备及应用系统的运行情况进行7\*24小时的不间断巡检监控，及时发现安全隐患，通知相关人员及时处理，并形成监控报告。每周反馈日志审计和数据库审计报告，进行总结分析。

（3）投标人需纳入行业监管部门网络安全保障整体工作体系，在涉及重保、安全事件、威胁情报等方面，配合安全服务商开展研判、处置、分析等工作。

（4）投标人承担云平台数据防篡改、防丢失的安全责任。业务数据未经采购人同意，不得离开云机房。投标人未经允许不得对云平台上的任何数据进行非法截取、加工、分析处理或提供给第三方机构。投标人在未经过用户邮件、书面材料确认前提下，不能查看、修改、拷贝用户业务系统文件和数据；各业务系统、数据归属于采购人，投标人无权支配。

（5）投标人需保证安全技术服务能力不低于所承载的信息系统的最高级别，并通过GB/T 22239相应等级的测评；符合GB/T 34080.1，GB/T 34080.2，GB/T 34080.3，GB/T 34080.4中的规定；通过商用密码应用安全性评估，商用密码应用安全性评估参考GB/T 39786-2021中相应等级规定；保障其上的租户安全、云主机安全、业务安全和数据安全；

（6）投标人应坚持制度和技术并重，建立健全网络和数据安全管理制度，落实网络和数据安全管理要求。采取相应技术措施，保障网络免受干扰、破坏或者未经授权的访问，防止数据泄露或者被窃取、篡改、破坏。

（7）对于关键信息基础设施，应当落实网络安全审查要求，采购网络产品和服务的，应当预判该产品和服务投入使用后可能带来的国家安全风险，确保采购国产化的网络产品和服务。影响或者可能影响国家安全的，应当申报网络安全审查。

（8）定期开展数据安全风险评估，发现数据安全隐患风险时，应当及时整改加固，采取必要的安全保护措施，防范数据安全风险。

（9）投标人应明确接触网络和信息系统、数据时的申请及审批流程，做好实名登记、权限控制、保密协议签署等管理。

（10）在服务期内，承载政务云平台的软硬件应在原厂维保期限内。

2.2.8运维服务

2.2.8.1服务内容

（1）负责云平台硬件资产、虚拟化资产的管理工作；

（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；

（3）执行云平台变更申请、审批流程；

（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；

（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。

2.2.8.2服务标准

（1）依据《北京市市级政务云管理办法》，投标人应当提供高效的系统维护服务，有效防范系统风险，系统对应负责人7\*24小时电话畅通，能够在系统发生除宕机外的其他故障问题时，能够协调人力资源在1小时内到达政务云机房现场提供服务。系统发生宕机问题时，投标人应在5分钟内响应，能够协调人力资源在1小时内到达运维现场定位、排除故障，在4个小时之内使系统恢复正常，故障处理完毕后提供相关系统宕机报告。

（2）为保障业务高峰期内系统平稳运行，缓解系统高峰期内因业务发生量增大而带来系统压力风险，要求投标人根据业务周期性特点，加大运维保障力度，保证在业务高峰期内系统平稳运行。

（3）重点保障时期重要信息系统云主机资源调整时间不超过4小时，针对重点保障时期的重要信息系统重要云主机，投标人应按采购人要求进行实时监控，超过预警阈值时主动上调云资源，并第一时间通知采购人进行相应操作，确保系统平稳运行。

（4）按照国家、北京市相关规定和信息安全技术标准及规范要求, 落实安全保障措施, 通过信息安全测评机构的测评和政务云安全审查 。

（5）投标人应明确运维操作规范和工作流程。定期开展文档查阅、漏洞扫描、渗透测试等多种形式的安全自查，排查政务网络和信息系统可能存在的安全漏洞，以及木马、后门、病毒等隐患风险，及时进行整改加固，切实防范安全风险。

（6）投标人应建立政务网络和数据安全监测通报机制，加强网络和数据安全监测，及时发布预警信息，开展政务网络和数据安全应急保障工作。发现其网络产品或服务存在安全漏洞等隐患风险时，应当立即采取补救措施，按照规定及时告知采购人并向有关监管部门报告。

（7）投标人应保障政务云规范运行。入云系统应开展网络安全测评及备案。应对数据进行分类分级管理，根据数据分级保护要求采取相应级别的安全防护措施；应按相关要求对重要数据进行异地备份。

（8）除不可抗力或计划内维护作业造成的政务云服务中断外,政务云实行24小时不间断运行。

2.2.9备份服务

9.1服务内容

投标人需具有本地和同城异地数据级备份能力，并配合采购人完成数据级容灾演练及恢复等工作。

9.2服务标准

按照采购人的各个应用系统对资源的备份需求通过备份策略实现对用户数据（文件、操作系统、数据库）的本地备份/异地备份（不包含备份存储空间费用），默认提供非结构化数据保护与文件备份保护。备份应满足如下要求:

（1）备份介质本身具备高可用性和冗余性。

（2） 备份方式包括完整备份、差异备份和增量备份。

（3）支持Windows系列操作系统、Linux主流系统操作系统、主流数据库软件、主流中间件软件、结构化数据以及非结构化数据等备份对象。

（4）支持建立统一的备份管理系统，用来管理本地备份和异地备份。

（5）投标人应提供对备份过程状态、备份结果提供运维监控保障服务，确保备份任务执行成功以及备份的数据完整性。

2.2.10日志服务

2.2.10.1服务内容

日志是发现问题、定位问题的重要信息，投标人提供统一的日志平台服务，针对操作系统进行日志收集，用于了解主机安全情况及资源使用情况，具体内容如下：

（1）支持的日志格式包括Web Service、Syslog、SNMP、JDBC、ODBC、HTTP/FTP、JASON等多种类型；

（2）支持通过统一的日志采集设备，对市级政务云内各类主机进行日志收集，并进行进一步的分析计算；

（3）支持结合威胁情报针对主机日志采集的高级威胁攻击进行检测；

（4）通过对主机日志数据分析，实现对用户和业务访问的精细化管理，建立网络流量的多种流量基线，从而为后续的链路、带宽和服务器扩容提供技术支撑；

（5）支持自定义日志副本数；

2.2.10.2服务标准

对主机系统日志进行采集分析处理，用于发现各种安全威胁、异常行为事件。主机系统日志应集中存储，且日志存储时间不低于6个月。

2.2.11迁移服务

2.2.11.1服务内容

如需迁移，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、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、配合架构规划设计、配合应用迁移部署等工作。

2.2.11.2服务标准

本项目涉及的业务系统为采购人在用的生产系统，目前在政务云上平稳运行，因此保障业务连续性是重要的保障需求。迁移服务具体要求如下：

（1）投标人需编制业务连续性服务方案。

（2）本项目如涉及系统迁移，在连续性服务方案中需提供确实可行的迁移部署服务子方案，迁移部署服务子方案应包括（但不限于）迁移部署流程（包含但不限于应用、虚拟机和数据类迁移）、业务系统部署迁移方案。迁移部署服务子方案应明确需要采购人配合的具体工作内容及时长，针对系统迁移过程中容易造成业务系统中断的环节，包含但不限于互联网及政务外网IP变更割接、业务数据同步及切换上线、应急回退方案等，进行风险评估，提出详细解决方案。

（3）本项目如涉及系统迁移，为保障业务系统的连续性，投标人应承诺自中标之日起，积极与原服务商对接，在20个工作日内，完成系统迁移平滑过渡，且因此产生的各项费用（包括但不限于测试阶段的云资源费用，系统开发商对业务系统的部署、调试费用等），应包含在投标人的报价中，提供“承诺函”并加盖投标人公章。

2.2.12其他服务

按照采购人的有关管理规定及具体需求提供个性化服务，包括密码应用安全支撑服务。

按照采购人有关国产密码应用改造等相关需求，提供咨询、评估、论证、使用等支撑保障服务，密码服务包括提供SSL证书、身份认证、数据加解密、数据安全传输 、签名验签、密钥管理等密码应用安全支撑服务。

2.3运维团队要求

（1）服务期内，投标人须设有7×24小时电话响应服务、具备运维团队，提供售后服务保障。团队成员应明确职责，架构清晰，岗位设置合理，且具备与本项目相关的项目经验。

（2）投标人须提供1名项目经理、1名安全技术负责人及4名项目团队专职人员，为本项目提供服务。项目经理及安全负责人需按照采购人要求，承担云资源服务保障具体工作，技术支持人员要求如下：

**服务团队人员要求**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 岗位 | 数量 | 学历 | 工作经验 | 岗位需具备的上岗资格证等要求 |
| 项目经理 | 1 | 本科及以上 | 有5年及以上类似工作经验 | 1、信息系统项目管理师2、信息安全保障人员认证证书（安全运维专业级或专业高级）3、信息安全保障人员认证证书（应急服务专业级或以上） |
| 安全技术负责人 | 1 | 本科及以上 | 有5年及以上类似工作经验 | 1、信息安全保障人员认证证书（安全集成专业级或以上）2、信息安全保障人员认证证书（应急服务专业级或以上）3、注册信息安全工程师证书（CISP） |
| 项目人员 | 4 | 本科及以上 | 有5年及以上类似工作经验 | 1、系统规划与管理师资质证书（高级）2、系统分析师资质证书（高级）3、系统架构设计师认证证书（高级）4、注册信息安全工程师证书（CISP） |

3. 验收标准

3.1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）。

3.2项目验收要求

（1）投标人所提供的北京市市级政务云基础资源服务应遵循客观、科学、合理的原则，符合《北京市市级政务云管理办法》的相关标准及要求。

（2）投标人所提供资源应满足采购文件规定的要求。保证合同期内系统安全稳定运行，不因硬件故障导致服务中断4小时及以上。

（3）服务期满后10个工作日开始对合同项目进行验收，投标人应当在采购人指定的验收日前向采购人提交验收报告。验收报告的内容包括但不限于，合同规定的各项服务清单，各系统设备运行情况。

（4）服务期届满，投标人按照采购人要求完成所有项目，各项记录、报告等文档齐全，无任何系统遗留问题，并通过由采购人组织的专家验收评审，方可通过验收。

4. 其他要求

4.1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）对于分包事项（如等保测评、密码应用安全性评估等），采购人应当对分包承接主体的网络安全能力进行评估，与网络服务提供者签订合同及保密协议，明确约定各方保障网络和数据安全的权利及义务。投标人应当具备网络和数据安全管理能力及相关资质，对提供产品和服务的安全性、合规性负责。发生网络安全事件时，在依法按程序报告的同时，投标人应当及时向采购人报告，并有义务配合调查。

（3）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。

4.2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。

4.3知识产权要求

（1）投标人应确保本项目所提交成果无知识产权纠纷，项目成果的知识产权属于项目委托方。须在响应文件中对此项作出专项承诺，格式自拟。

（2）投标人保证向采购人提供的服务成果是其独立实施完成，不存在任何侵犯第三方专利权、商标权、著作权等合法权益。如因投标人提供的服务成果侵犯任何第三方的合法权益，导致该第三方追究采购人责任的，投标人应负责解决并赔偿因此给采购人造成的全部损失。