**采购需求**

# 项目概况

按照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》（京经信委函〔2019〕150号）关于“上云为常态、不上云为例外”的要求，我单位现有信息系统北京市城市管理综合执法大数据平台（以下简称“平台”）自2021年起迁入市政务云。本项目租用市政务云资源，为平台提供运行所需的计算、存储、网络带宽、主机深度监控等服务，保障平台安全稳定运行。

# 采购目标

本项目的总体目标是通过租用政务云服务，对市城管执法局云上业务系统的运行环境进行持续优化，提供可靠、稳定、安全的政务云服务，具体包括：

1.提供市级政务云平台的计算、存储、网络、安全等服务，完成云上业务系统运行环境的日常运维、安全运维、应急响应等工作，确保云上业务系统安全、稳定运行。

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，确保云上业务系统在政务云环境中可靠稳定运行。

# 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/T 22240-2020）

《信息安全技术 网络安全等级保护实施指南》（GB/T 25058-2019）

《信息安全技术 网络安全等级保护安全设计技术要求》（GB/T 25070-2019）

《信息安全技术 网络安全等级保护基本要求》（GB/T 22239-2019）

《信息安全技术 网络安全等级保护测评要求》（GB/T 28448-20190）

《信息安全技术 网络安全等级保护测评过程指南》（GB/T 28449-2018）

《信息安全技术 网络安全等级保护测试评估技术指南》（GB/T 36627-2018）

《信息安全技术 信息系统密码应用基本要求》（GB/T 39786-2021）

《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》（GB 50174-2017）

《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》

**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》

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。

# 四、技术要求

投标人应按下表数量需求和采购人具体要求提供市级政务云服务。

**政务云服务需求数量详表**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 序号 | 服务大类 | 服务子类 | 服务项 | 计价单位 | 报价单位 | 数量 | 服务期（月） |
| 1 | 云主机服务 | x86平台云主机服务 | vCPU（主频不低于2.4GHz） | 1CPU | 元/月 | 4235 | 12 |
| 2 | 内存 | 1GB | 元/月 | 9269 | 12 |
| 3 | 存储服务 | 存储服务-普通 | 提供普通性能存储服务（单盘IOPS 2000-5000） | 1GB | 元/月 | 358742 | 12 |
| 4 | 存储服务-高性能 | 提供高性能存储服务（单盘IOPS 10000-25000） | 1GB | 元/月 | 149938 | 12 |
| 5 | 存储服务-高性能对象存储 | 提供高性能对象存储服务（单盘IOPS 10000-25000） | 1GB | 元/月 | 30000 | 12 |
| 6 | 静态存储 | 大容量、高可靠的数据存储服务，具备PB级线性扩展能力 | 1TB | 元/月 | 53 | 12 |
| 7 | 网络服务 | 互联网链路带宽 | 须提供多线运营商接入服务，保证稳定可靠。 | 1Mb | 元/月 | 300 | 12 |
| 8 | 互联网IP地址服务 | 提供互联网地址租用，并且提供网站域名备案服务。 | 1IP | 元/月 | 7 | 12 |
| 9 | 负载均衡 | 主机负载均衡服务 | 1IP | 元/月 | 27 | 12 |
| 10 | 远程接入服务 | 每个账号结合身份验通过VPN远程接入堡垒机维护 | 1账号 | 元/月 | 33 | 12 |
| 11 | SSL证书 | 提供SSL证书服务，提供https保护，对流量进行加密，防止数据被窃取。 | 1套 | 元/月 | 2 | 12 |
| 12 | 备份服务 | 本地备份服务 | 通过备份策略实现文件、操作系统、数据库的本地备份（不包含备份存储空间费用） | 1GB | 元/月 | 53000 | 12 |
| 13 | 基础软件支撑服务 | Windows Server 套餐 | Windows Server 租用、安装及维护。 | 1套 | 元/月 | 28 | 12 |
| 14 | 开源操作系统套餐 | 开源操作系统租用、安装及维护。 | 1套 | 元/月 | 228 | 12 |
| 15 | 国产操作系统套餐 | 国产化要求操作系统套餐服务-统信 | 1套 | 元/月 | 9 | 12 |
| 16 | 安全服务 | WAF防护 | WAF防护服务，保证用户网站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，可起到前端防护作用。 | 1IP | 元/月 | 7 | 12 |
| 17 | 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。 | 1套 | 元/月 | 2 | 12 |
| 18 | 云端抗DDOS服务 | 提供云端抗DDOS服务，避免业务遭受拒绝服务攻击 | 1套 | 元/月 | 1 | 12 |
| 19 | 主机杀毒服务 | 对云主机进行定期的病毒查杀，杀毒软件集中控制，对网络性能无影响。 | 1台 | 元/月 | 265 | 12 |
| 20 | 支持国密远程运维接入（含usbkey、VPN） | 支持国密远程运维接入服务，仅包含绑定国密数字证书usbkey 1个）及支持国密VPN运维通道 | 1套 | 元/月 | 1 | 12 |
| 21 | 运维服务 | 云主机深度监控服务 | 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 | 265 | 12 |
| 22 | 其他服务 | CDN服务 | 将源站内容分发至最接近用户的节点，使用户可就近取得所需内容，提高用户访问的响应速度和成功率。 | 1月 | 元/月 | 20000 | 12 |

## （一）云主机服务

**1.1服务内容**

按照采购人的数量需求，提供云主机服务，包括：x86平台云主机服务、国产芯片云主机服务等，在提供政务云主机的服务过程中做好与采购人和信息系统服务商的协调沟通工作，并按照采购人要求对 vCPU 及内存进行动态调整，实现合理的计算资源配置，自接到工单至完成调整时间不超过 4 小时。

**1.2服务标准**

1.2.1 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；

1.2.2 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；

1.2.3 应满足云主机之间、CPU之间隔离保护要求；

1.2.4 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；

1.2.5 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；

1.2.6 支持异构虚拟化能力，如KVM、PowerVM等多种虚拟化技术；

1.2.7 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；

1.2.8 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；

1.2.9 云服务可用性不低于99.99%

## （二）存储服务

**2.1服务内容**

按照采购人的数量需求，提供存储服务，包括：普通性能存储、高性能存储、静态存储，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，并按照采购人要求对存储配置进行动态调整，其中增加存储配置的调整用时不超过 4 小时，降低存储配置的调整用时不超过 8 个小时，实现合理的存储资源配置。

**2.2服务标准**

2.2.1 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；

2.2.2 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；

2.2.3 支持存储资源扩展能力，例如：PB级扩展；

2.2.4 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；

2.2.5 支持加密存储，使用的密码算法应符合法律、法规的规定和密码相关国家标准、行业标准的有关要求；

## （三）网络服务

**3.1服务内容**

按照采购人的具体需求，提供网络服务，主要内容包含：

3.1.1 提供互联网 IP 地址租用及链路带宽服务，做好配套的 IP 地址备案、网络策略配置 工作。

3.1.2 提供主机负载均衡服务，采用全冗余或集群架构，保证无单点故障。

3.1.3 提供远程接入服务，进行远程接入账户管理，实现通过 VPN 访问系统及数据传输等功能。

3.1.4 提供SSL证书服务，保证系统数据的SSL加密传输。

**3.2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：

3.2.1 具备多运营商网络接入服务的能力；

3.2.2 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；

3.2.3 应采用集群部署网络控制，以保障升级时业务不中断；

3.2.4 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；

3.2.5 支持IPv6地址分配，满足业务系统IPv6要求；

3.2.6 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；

3.2.7 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；

3.2.8 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。

3.2.9 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；

3.2.10 远程接入服务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。

3.2.11 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。

3.1.12 SSL证书服务须支持服务器、负载均衡等设备部署配置，实现数据信息在客户端和服务器之间的加密传输，可以防止数据信息的泄露，保证信息传递的安全性。

## （四）备份服务

**4.1服务内容**

按照采购人的具体需求，提供备份服务，投标人需具有本地和同城异地数据级备份能力，在采购人有需要时配合完成数据级容灾演练及恢复等工作。

**4.2服务标准**

按照采购人的业务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（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:

4.2.1 备份介质本身具备高可用性和冗余性。

4.2.2 备份方式包括完整备份、差异备份和增量备份。

4.2.3 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。

4.2.4 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。

4.2.5 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。

4.2.6 备份策略及备份频率不得低于每天一次增量备份，每周一次全量备份。要求政务云扩展服务与基础服务紧密配合，确保入云系统正常稳定运行。

## （五）基础软件支撑服务

**5.1 服务内容**

按照采购人的具体需求，提供商用操作系统、开源操作系统等软件支撑服务。

**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，支持Windows Server、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。

5.2.2 开源操作系统套餐

提供主流开源操作系统服务，支持CentOS、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。

## （六）安全服务

**6.1 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。主要内容包含：

6.1.1 基础安全保障服务

云服务商应按照《北京市市级政务云管理办法》的要求免费提供编号为 3001-3015 的安全管理服务和安全技术服务。

6.1.2 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。

6.1.3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。

6.1.4 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。

6.1.5 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。

**6.2服务标准**

6.2.1 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。投标人本次项目提供服务的云平台应通过网络安全等级保护（GB/T 22239-2019）第三级测评，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。投标人须提供近一年内通过网络安全等级保护（GB/T 22239-2019）第三级的测评报告（至少包括报告首页、网络安全等级测评基本信息表页、等级测评结论页），评测报告持有人与投标人必须完全一致，

6.2.2 投标人需利用监控系统或人工对机房环境、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。

6.2.3 投标人需纳入行业监管部门网络安全保障整体工作体系，同时在涉及重保、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。投标人本次项目提供服务的云平台须通过《中央网信办云计算服务安全评估》并提供中央网信办网站公示截图，单位名称须与投标人名称完全一致，以证明投标人具备提高云计算服务的安全可控水平，降低云计算服务带来的网络安全风险的能力。

6.2.4 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。

6.2.5 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、容器安全、云主机安全、业务安全和数据安全。投标人应提供一年内云平台商业密码安全性评估报告关键页（至少包括报告首页、被测系统基本信息表页、商用密码应用安全性评估结论页），评估结果符合密评第三级信息系统要求，评测报告持有人与投标人必须完全一致。

6.2.6 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。

6.2.7 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，确保采购安全可信的网络产品和服务。影响或者可能影响国家安全的，应当申报网络安全审查。

6.2.8 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。

6.2.9 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。

6.2.10 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。

## （七）其他服务

投标人应提供以下服务：

7.1 提供日志服务，投标人应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。

7.2 提供业务系统迁移服务，本项目涉及的业务系统目前在北京市政务云上平稳运行，投标人需按以下要求提供相关证书和“承诺函”：

7.2.1 投标人需具备有效的业务连续性管理体系认证。提供相关证书复印件，证书单位名称须与投标人名称完全一致。

7.2.2 投标人应承诺负责云资源配置、应用迁移、数据迁移、测试验证、业务割接、安全和应急保障等工作，迁移不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，如因系统迁移导致采购人系统损坏、数据丢失，一切后果均由投标人承担。

7.2.3 为保障业务系统的连续性，投标人应承诺自行承担产生的各项费用（包括但不限于迁移及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，原有云服务商配合迁移产生的费用等）。同时，投标人应承诺，如无法按采购人要求完成迁移工作，采购人有权解除合同，并要求投标人赔偿相应违约金和经济损失。

7.2.4 为满足业务连续性和不可中断的要求，投标人应承诺，本项目服务期限届满后，若涉及系统迁移工作，投标人积极配合下年中标人开展迁移工作。

7.2.5 为保障业务系统的连续性，投标人应承诺自中标之日起，积极与原云服务商对接，在1个工作日内（含1个工作日），且因迁移导致的业务系统运行中断6小时以内（含6小时），完成系统迁移平滑过渡。

## （八）运维服务要求

**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 负责信息系统入云、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 负责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。投标人需针对采购人要求的云平台运维服务相关内容，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。

8.1.6 投标人应提供高效的故障响应及处置服务，有效防范系统风险，建立服务热线或指定专人受理采购人提出的各类故障申告，保证7×24小时电话畅通。

8.1.7 投标人须提供春节、两会、国庆等节假日、重要会议、重大活动等重要时间点的重保服务，加大运维保障力度，保证重点时期业务系统安全平稳运行。

8.1.8 提供云主机深度监控服务，投标人应在主机中部署探针深度监测主机运行情况。提供7x24小时运维值守、30分钟内应急响应，不仅限于机房巡检、云平台和硬件监控，同时提供应急问题排查协助、协助处理应用故障等服务，并提供相关报告。

8.1.9 投标人应强化云资源使用情况的监测与分析，建立云资源调整协同工作机制，对监测发现的CPU、内存、存储等过高或过低情况，应及时向采购人提交提交云资源优化建议，并主动配合云资源实施弹性扩缩容、负载均衡调整等云资源优化措施。

**8.2 服务标准**

8.2.1 投标人须严格按照《北京市市级政务云管理办法》，以及采购人制定的管理办法及流程等相关制度，开展标准化运维工作。

8.2.2 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。

8.2.3 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。

8.2.4 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。

8.2.5 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。

8.2.6 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。

8.2.7 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备份。

8.2.8 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。

8.2.9 投标人须每月提供政务云运维月报，对当月政务云服务情况进行总结，包括各类云资源调整、使用及服务情况，以及日常维护、应急值守、故障及安全事件处置等情况。

8.2.10 投标人需提供运维服务方案，包含运维服务制度、规范、流程；业务系统运行可靠性保障方案；有利于运维服务的合理化建议等。

8.2.11 投标人须提供故障响应及处置服务方案，充分分析可能出现的各类故障，并提出合理可行保障措施。

8.2.12发生故障时，投标人应在故障响应时间在15分钟内响应，30分钟内进行完成故障定位排除。发生系统宕机问题时，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。投标人须按上述要求，明确故障响应及处置时间，并提供故障响应及处置承诺函。

8.2.13 投标人须提供重保服务方案，包含重要时间节点如春节、两会、国庆等节假日、重要会议、重大活动等时间点，加大运维保障力度，保证重点时期业务系统安全平稳运行。

8.2.14 投标人需具备有效的质量管理体系认证、信息安全管理体系认证、信息技术服务管理体系认证。提供相关证书复印件，证书单位名称须与投标人名称完全一致。

## （九）服务团队要求

9.1 投标人需提供1名项目经理。项目经理需具备有5年及以上类似工作经验，具备信息系统项目管理师（高级）证书（投标人提供身份证复印件、证书复印件、人员简历（形式不限）等材料）。

9.2 投标人需提供1名技术负责人。技术负责人具有5年及以上从事云技术服务或类似工作经验。（投标人提供身份证复印件、证书复印件、人员简历（形式不限）等材料）。

9.3投标人需提供不少于4人的服务团队（不含项目经理和技术负责人），拟派团队成员应具备CISP证书、网络规划设计师（高级）证书、信息系统项目管理师证书、数据库系统工程师证书。（投标人需提供人员身份证复印件、证书复印件、人员简历（形式不限），否则不予认可）。

# 五、商务要求

## （一）服务地点

北京市政务服务中心六里桥机房，必要时到采购人办公现场提供技术支持服务。

## （二）服务期限

2025年6月27日至2026年6月26日，共12个月。

## （三）支付方式

合同签订后1个月内支付项目首款（2025年当年项目预算批复资金的50%）；2025年第三季度结束前支付项目第二笔款（2025年当年项目预算批复资金的40%）；2025年第四季度结束前支付项目第三笔款（支付2025年当年项目预算批复资金的10%）；2026年第一季度结束前，支付项目第四笔款（合同剩余款项的60%）；项目通过验收后，支付合同尾款。支付方式详见合同。

## （四）验收服务标准

1.服务绩效指标

（1）云服务可用性不低于99.99%；

（2）故障及安全事件响应率达到100%；

（3）全年重大责任安全事件次数为0次；

（4）故障及安全事件响应时间小于15分钟；

（5）故障定位排除时间小于30分钟；

（6）业务系统入云率等于100%;

（7）使用人员满意度不低于95%。

2.项目验收要求

2.1阶段查验：投标人需在次月中旬前提供完整的上月/季度工作资料（包括但不限于月报、重保记录、工单、故障及安全事件处置记录、满意度评价表等），采购人定期对服务情况进行评估及查验。

2.2项目验收：服务期到期后，投标人应及时通知采购人进行验收。采购人通过审核服务任务完成数量、质量、项目文档材料的方式开展项目验收。

2.3具体时间和地点由双方商议安排，出具书面意见。

2.4验收具体时间和地点由双方商议安排，出具书面意见。

2.5对于项目验收结果未通过的情况，由投标人按照验收意见采取补救措施后再次进行验收直至通过项目验收，由此产生的全部费用均由投标人承担。