**第五章 采购需求**

1. **、项目背景**

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）等文件的要求，北京市统计局开展2025年市级政务云服务项目采购，确保云上信息系统在政务云环境下可靠稳定安全运行。

1. **、技术参数要求**
   1. **政务云基础服务**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **服务类别** | **服务子类** | **服务项** | **计价单位** | **报价单位** | **数量** | **期限（月）** |
| **计算服务** | 平台云主机服务（包含X86、ARM、C86） | vCPU（vCPU ARM架构主频不低于2.4GHz，C86和X86主频不低于2.2GHz，平均虚拟化率，即物理CPU/虚拟CPU≥1/4，虚拟CPU利用率不低于物理CPU的25%） | 1 CPU | 元/月 | 1665 | 12 |
| 内存 | 1 GB | 元/月 | 6103 | 12 |
| 物理服务器租用服务（包含X86、ARM、C86） | 配置1：双路每CPU核数≥32核，主频≥2.0GHz，128G内存，2块600G SAS硬盘，2个HBA卡，2个万兆端口 | 1 台 | 元/月 | 6 | 12 |
| 内存-32GB内存 | 1 条 | 元/月 | 168 | 12 |
| 硬盘配置1-480GB SSD | 1 块 | 元/月 | 88 | 12 |
| **存储服务** | 普通性能存储 | 普通存储（单盘技术指标: 单盘IOPS 1000-3000 ） | 1 GB | 元/月 | 90224 | 12 |
| 高性能存储 | 高性能存储（单盘技术指标：单盘IOPS 3000-20000 ） | 1 GB | 元/月 | 68826 | 12 |
| 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，提供静态数据存储 | 1 TB | 元/月 | 6 | 12 |
| 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） | 1 GB | 元/月 | 90224 | 12 |
| **网络服务** | 互联网链路服务 | 互联网链路带宽 | 1 Mb | 元/月 | 500 | 12 |
| 互联网IP地址租用服务、并提供备案服务 | 1 IP | 元/月 | 8 | 12 |
| 主机负载均衡服务 | 主机负载均衡服务 | 1 IP（内网） | 元/月 | 40 | 12 |
| 远程接入服务 | 每个账号结合身份验证通过VPN远程接入堡垒机进行维护 | 1账号 | 元/月 | 54 | 12 |
| WAF防护 | 在网站前端架设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 | 1 IP（互联网） | 元/月 | 7 | 12 |

* 1. **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** | **期限（月）** |
| **安全服务** | 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 | 86 | 12 |
| 主机防护 | 主机防护：提供符合等保三级要求的主机权限管理及安全防护 | 1台 | 元/月 | 86 | 12 |
| **安全检测监测、审计服务** | 主机日志分析 | 针对操作系统进行日志收集，并且进行分析，并将结果反馈给用户，用于了解主机安全情况及资源使用情况 | 1台 | 元/月 | 86 | 12 |
| 数据库审计服务 | 支持Oracle及相关国产数据库审计。（1套为1个数据库实例） | 1套 | 元/月 | 24 | 12 |
| **国密服务** | 强身份认证服务 | 为系统提供强身份认证服务，基于数字证书登录业务系统 | 1套 | 元/月 | 1 | 12 |
| 签名验证服务 | 为系统提供重要数据在存储、传输过程中的完整性保护 | 1套 | 元/月 | 1 | 12 |
| 加解密服务 | 为系统提供重要数据在存储、传输过程中的机密性保护 | 1套 | 元/月 | 1 | 12 |
| 时间戳服务 | 为系统提供重要数据在不可否认性保护 | 1套 | 元/月 | 1 | 12 |
| SSL安全服务 | 基于SM2/SM3/SM4算法建立SSL通信信道，保证通信过程中数据的机密性和完整性 | 1套 | 元/月 | 2 | 12 |
| 云服务接入集成费 | 提供应用系统接入云服务所需应用集成、开通和配置服务 | 1套 | 个 | 1 | / |
| 国密浏览器 | 1.支持SM2/SM3/SM4国密算法以及国密的SSL双向协议；2.支持国密网站、国密应用自动识别及国密标识展现；3.支持国产系列操作系统，如中标麒麟、银河麒麟、中科方德、UOS；4.支持国产系列（包括龙芯（MIPS）、兆芯、飞腾（ARM）、海光）等各架构CPU；5.支持页面解析、页面标签栏、页面地址栏、前进后退、页面刷新、网址收藏、证书集成、插件集成等浏览器功能；6.支持安全沙箱、环境检查、完整性校验、隐私设置、无痕浏览、缓存加密、反调试及证书管控、插件管控等安全性功能。 | 1用户 | 元/月 | 5 | 12 |
| 设备证书 | 标识各类设备的网上身份 | 1年 | 张 | 25 | / |
| **其他服务** | 短信服务 | 提供短信验证服务 | / | 元/条 | 700000 | / |
| 国产商用操作系统租用 | 国产商用操作系统租用、安装、调优，排错，技术支持 | 1台 | 元/月 | 44 | 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 | 1CPU | 元/月 | 22 | 12 |
| 国产商用数据库套餐 | 国产数据库租用、安装及原厂技术支持服务 | 1套 | 元/月 | 5 | 12 |
| 高斯测试数据库安装及原厂技术支持服务 | 1节点 | 元/月 | 3 | 12 |
| 高斯数据库租用、安装及原厂技术支持服务 | 1节点 | 元/月 | 3 | 12 |
| 商用数据库租用服务 | Oracle12C 标准版（不含RAC组件）租用、安装、维护服务 | 1套 | 元/月 | 2 | 12 |

1. **、采购目标**

本项目的总体目标是通过租用政务云平台计算服务、存储服务、网络服务、安全服务、安全检测监测、审计服务、国密服务及其他服务等。提供全年7×24小时运维保障，做好法定节假日和重点时期应急值守保障服务，确保各信息系统在政务云环境中安全稳定运行。

1. **、服务内容与服务标准**
   1. **计算服务**
      1. **服务内容**

按照采购人的具体需求，提供计算服务，包括：平台云主机服务和物理服务器租用服务，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. **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。
       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：

（1）物理服务器CPU主频应不低于2.40GHz；

（2）主机内存硬件配置不低于DDR4-2400MHz；

（3）可用性不低于99.9%。

* 1. **存储服务**
     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、静态存储服务，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。

* + 1. **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：

(1)吞吐量：高性能存储系统的读写带宽应不低于1000MB/s，IOPS不低于20000；普通性能存储系统的读写带宽应不低于200MB/s，IOPS不低于1000。

(2)支持高可靠性，可靠性不低于99.9%。

* 1. **备份服务**
     1. **服务内容**

按照采购人的具体需求，提供本地备份服务，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。

* + 1. **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（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. 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。
  1. **网络服务**
     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，按照采购人的具体需求，提供主机负载均衡服务。
        3. 远程接入服务，提供远程接入服务，每个账号结合身份验证接入堡垒机维护应用系统。
        4. WAF防护服务，按照采购人的具体需求，提供WAF防护服务，在政务云流量入口架设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. **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. 应采用集群部署网络控制，以保障升级时业务不中断。
      3. 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。
      4. 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。
      5. 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。
      6. 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。
      7. 网络系统性能要求包括但不限于如下：

（1）云内骨干线路带宽不低于10Gb/s；

（2）服务器业务带宽不低于1Gb/s；

（3）平均可用性不低于99.9%。

* 1. **安全及安全检测监测、审计服务**
     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等要求建设安全技术防护体系和安全管理体系，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. 主机杀毒服务

按照采购人的具体需求，提供主机杀毒服务，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. 主机防护

按照采购人的具体需求，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。

* + - 1. 主机日志分析

按照采购人的具体需求，投标人需提供主机日志分析服务。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，日志存储时间不低于1年，并根据要求提供主机日志分析报告。

* + - 1. 数据库审计服务

按照采购人的具体需求，投标人需提供数据库审计服务。实时进行数据库访问监视与审计，为事后追查提供可靠的依据和来源，审计内容包括但不限于：发生时间、源IP、源端口、源MAC、目的IP、目的端口、数据库用户、数据库类型、操作类型、SQL语句、SQL模版、客户端程序名、响应码、影响行数、返回行数、SQL预计响应时间等。支持对Oracle和高斯等数据库审计，审计日志存储时间不低于1年，可根据要求提供数据库审计报告。

* + 1. **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，并形成监控报告。定期反馈日志分析和数据库审计报告，进行总结分析。
       3. 投标人需纳入政务云监管单位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/T22239相应等级的测评；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/T39786-2021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。
  1. **国密服务及其他服务**
     1. **服务内容**

为本项目提供的国密服务包含：强身份认证服务、签名验证服务、加解密服务、时间戳服务、SSL安全服务、云服务接入集成费、国密浏览器和设备证书服务；其他服务包含：短信服务、国产商用操作系统租用、国产商用中间件套餐、国产商用数据库套餐和商用数据库租用服务。

* + 1. **服务标准**
       1. 强身份认证服务

按照采购人的具体需求，为系统提供强身份认证服务，基于数字证书登录业务系统，需采用基于数字证书的强身份认证服务满足用户的身份认证需求，完善身份认证的环节，确保身份认证安全可信。

* + - 1. 签名验证服务

按照采购人的具体需求，为系统提供重要数据在存储、传输过程中的完整性保护，需对业务应用提供数据签名、签名验证等服务，确保数据的真实性、完整性和不可抵赖性。

* + - 1. 加解密服务

按照采购人的具体需求，为系统提供重要数据在存储、传输过程中的机密性保护，需对业务数据提供加解密服务，确保数据传输过程的机密性。

* + - 1. 时间戳服务

按照采购人的具体需求，为系统提供重要数据在不可否认性保护，以API方式提供密码服务，计算资源由云端统一保障。

* + - 1. SSL安全服务

按照采购人的具体需求，提供SSL安全服务，需采用国产算法SSL建立https通信，实现信息传输通道加密。

* + - 1. 云服务接入集成费

按照采购人的具体需求，提供应用系统接入云服务所需应用集成、开通和配置服务。密码云接入服务包括对云签名服务、时间戳服务和证书服务等服务的集成和配置。

* + - 1. 国密浏览器

按照采购人的具体需求，提供国密浏览器服务，由浏览器内核、浏览器界面、密码算法SSL协议逻辑运算模块、智能密码钥匙等组成。支持SM2/SM3/SM4算法与WEB服务器之间建立安全通道，保证WEB网页访问的安全性。

* + - 1. 设备证书服务

按照采购人的具体需求，提供设备证书服务，用于标识各类设备的网上身份。

* + - 1. 短信服务

按照采购人的具体需求，为云上系统提供互联网/政务外网环境的短信服务，通过API接口方式接入政务云平台。

* + - 1. 国产商用操作系统租用

按照采购人的具体需求，提供统信和麒麟等国产操作系统租用、安装及原厂技术支持服务。

* + - 1. 国产商用中间件套餐

按照采购人的具体需求，提供国产商用应用中间件租用、安装及原厂技术支持服务。

* + - 1. 国产商用数据库套餐

按照采购人的具体需求，提供国产数据库、高斯测试数据库、高斯数据库租用、安装及原厂技术支持服务。

* + - 1. 商用数据库租用服务

按照采购人的具体需求，提供oracle12C标准版（不含RAC组件）租用、安装及原厂技术支持服务。

* 1. **运维服务**
     1. **服务内容**
        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。
        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。
        6. 提供服务器资源监测及预警服务，实时做好资源的动态监控工作，为资源使用情况设置阈值，达到阈值时，及时建议采购人实施资源动态调整。每月向采购人提供资源使用情况报告，结合实际给出合理性建议。对采购人提出的资源申请工单进行合理性评估。
        7. 辅助做好网络安全监测、检测服务，从网络层到应用层进行全面扫描和查杀，对各种加壳、压缩、加密病毒，以及木马、蠕虫、恶意软件等网络威胁均能够快速、准确地彻底清除。同时可依托云平台安全态势感知能力提供业务可视化、威胁可视化、攻击与可疑流量可视化服务，在系统存在弱口令或受到威胁入侵之后，损失发生之前及时发现威胁，可直观看到网络攻击情况，服务按月度产出服务报告。
     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20分钟内响应，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1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. 投标人负责对云资源使用情况进行监控，发生云资源使用率过高情况时应及时通知采购人。每月提供政务云服务报告，需要涉及云资源使用情况，统计各信息系统云效率，针对云效率情况提供资源调整建议。
        5. 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。
        6. 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. **迁移服务**
     1. **服务内容**

投标人需提供整体的业务上云迁移服务，应支持云主机迁移、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。

* + 1. **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，目前在北京市政务云上平稳运行，因此业务连续性是首要的保障需求。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5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。

1. **、运维团队要求**

投标人需针对本项目设立项目团队，项目团队人数应不少于10人，需提供团队组织架构、成员名单及职责（加盖投标人单位公章）。

投标人承担该项目的项目经理应同时具有信息系统项目管理师证书（需提供证书扫描或复印件并加盖投标人公章）。

投标人提供安全运维工程师不少于2名，具有五年及以上安全运维相关从业经验，提供个人简历、项目经历材料（加盖投标人单位公章）。

投标人提供数据库运维工程师不少于1名，具有五年及以上数据库运维相关从业经验，提供个人简历、项目经历材料（加盖投标人单位公章）。

投标人提供网络运维工程师不少于3名，具有五年及以上网络运维相关从业经验，提供个人简历、项目经历材料（加盖投标人单位公章）。

投标人提供平台运维工程师不少于2名，具有五年及以上云平台运维相关从业经验，提供个人简历、项目经历材料（加盖投标人单位公章）。

1. **、商务要求**
   1. **服务地点**

采购人指定。

* 1. **服务期限**

自合同签订之日起12个自然月。

* 1. **支付方式**

合同签订之日起20个工作日内，支付服务费的80%；项目通过验收后20个工作日内，支付服务费的20%，支付方式详见合同。

* 1. **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）。

* + 1. **项目验收要求**

（1）投标人所提供的北京市市级政务云服务应遵循客观、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招标文件规定的要求。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12小时及以上。

（3）服务期满后30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。

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从合同签订之日起永久有效，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。

1. **、政策性采购需求**

为在项目中充分落实《政府采购法》规定的“政府采购应当有助于实现国家的经济和社会发展政策目标”等相关要求，以项目为载体推动北京市环境社会治理(ESG)体系高质量发展，请供应商提供在本项目中落实ESG理念的工作措施。

1. **、其他相关要求**

（1）投标人在2022年7月至投标文件递交截止日应承担过与本项目类似的项目，并提供业绩证明材料。业绩证明材料指合同复印件，合同复印件至少包含首页、主要内容页、签字盖章页。

（2）本项目所需政务云平台需通过网络安全等级保护三级测评、商用密码应用安全性评估及中央网信办云计算服务安全评估，能够提供相关证明并加盖投标人公章。