**第五章 采购需求**

**一、采购标的**

## **1.采购标的**

项目名称：北京市市场监督管理局2025-2026年政务云基础资源租用服务项目

标的名称：北京市市场监督管理局2025-2026年政务云基础资源租用服务项目

项目预算：548.152533 万元。

合同履行期限：自合同签订之日起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北京市综合监管信息系统、北京市市场监督管理局事中监管系统、北京市法人基础信息数据库、北京市平台经济综合监管服务系统、北京市市场监督管理局产品质量监督业务管理平台、北京市商务楼宇信息监测系统、北京市市场监督管理局人力资源管理系统、北京市市场监督管理局数据中心系统、北京市市场监督管理局网站系统、北京市市场监督管理局综合财务管理信息系统、北京市计量器具管理系统、北京市市场监督管理局企业信用信息公示系统、北京市市场监督管理局市场主体网格监管系统、北京市企业网上年度申报系统、北京市市场监督管理局特种设备管理综合业务平台、北京市市场监督管理局广告监测系统、北京市市场监督管理局综合执法办案平台、北京市企业登记e窗通服务平台、北京市市场监督管理局企业档案信息综合安全管理系统、北京市统一社会信用代码数据库、北京市标准化管理信息系统共21个政务信息系统自2019年起迁入市政务云。

**二、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：自合同签订之日起12个月。

## **2. 付款条件（进度和方式）**

本项目按合同总金额30%、45%、25%的比例支付首款、中期款、尾款（服务期满后）。

**三、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，对北京市市场监督管理局业务信息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、日常运行维护、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

1.2.1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）

1.2.2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 28448-2019）

《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》

1.2.3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。**

## **2. 服务内容及要求**

2.1采购服务清单

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **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）** |
| 计算服务 | x86平台云主机服务 | vCPU（主频不低于2.4GHz） | 1CPU | 元/月 | 4838 | 12 （584个CPU为11个月20天） |
| 内存 | 1GB | 元/月 | 10732 | 12 （1840个GB为11个月20天） |
| 存储服务 | 普通性能存储 | 普通存储（单盘技术指标:单盘IOPS2000-5000） | 1GB | 元/月 | 112514 | 12 （12000个GB为11个月20天） |
| 高性能存储 | 高性能存储（单盘技术指标：单盘IOPS10000-25000） | 1GB | 元/月 | 384336 | 12 （36800个GB为11个月20天） |
| 网络服务 | 互联网链路服务 | 互联网链路带宽 | 1Mb | 元/月 | 1250 | 12 （170Mb为11个月20天） |
| 互联网IP地址租用服务、并提供备案服务 | 1IP | 元/月 | 23 | 12 （4个IP为11个月20天） |
| 主机负载均衡服务 | 主机负载均衡服务 | 1IP（内网） | 元/月 | 92 | 12 |
| 远程接入服务 | 远程接入服务 | 1账号 | 元/月 | 41 | 12 （4个VPN账号为11个月20天） |
| VPN服务 | SSL VPN接入 | 1套 | 元/月 | 40 | 12 （3个VPN账号为11个月20天） |
| IPSec VPN接入 | 1套 | 元/月 | 58 | 11个月20天 |
| WAF防护 | web应用防火墙服务 | 1IP（互联网） | 元/月 | 23 | 12 （4个VPN账号为11个月20天） |
| 云主机深度监控服务 | 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 | 219 | 12 （58台为11个月20天） |

2.2服务标准要求

2.2.1云主机服务

|  |  |
| --- | --- |
| 指标项 | 规格要求 |
| 性能限制 | 按内存不复用方式分配资源，要求CPU主频≥2.4GHz |
| 性能范围 | CPU核数可选范围1-16核，内存可选范围1-64G |
| 操作系统兼容性 | 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 |
| 扩展性 | 用户可以灵活调整云主机CPU、内存、硬盘规格 |
| 云主机隔离 | 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。 |
| 管理权限 | 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。 |
| HA功能 | 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 |
| 备份功能 | 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 |
| 可操作性 | 支持通过云管理平台，实现申请部署与使用 |
| 安全防护 | 提供防ARP欺骗、自定义防火墙功能，支持防DDos攻击； |
| 弹性网络 | 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； |
| 镜像快照 | 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。 |
| 数据存储 | 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%； |
| 高可用性 | 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%； |
| 扩展性 | 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； |

2.2.2存储服务

**1、普通性能存储服务**

|  |  |
| --- | --- |
| 指标项 | 服务要求 |
| 可靠性要求 | 提供普通存储服务，要求稳定可靠，确保数据可靠性99.9999% |
| 性能要求 | 单盘技术指标满足IOPS 2000-5000 |
| 使用要求 | 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 |
| 架构要求 | 系统整体架构无单点故障 |
| 可操作性 | 支持通过云管理平台，实现申请部署与使用 |

**2、高性能存储服务**

|  |  |
| --- | --- |
| 指标项 | 服务要求 |
| 可靠性要求 | 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% |
| 性能要求 | 单盘技术指标满足IOPS 10000-25000 |
| 使用要求 | 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 |
| 架构要求 | 系统整体架构无单点故障 |
| 可操作性 | 支持通过云管理平台，实现申请部署与使用 |

2.2.3网络服务

**1、互联网链路服务**

|  |  |
| --- | --- |
| 指标项 | 服务要求 |
| 带宽租用服务 | 提供互联网带宽租用服务，带宽提供方应为一级运营商 |
| 可靠性要求 | 须提供多线运营商接入服务，保证服务稳定可靠。 |
| 可操作性 | 支持通过云管理平台，实现申请部署与使用 |
| 互联网IP地址租用服务 | 可提供IPV4/IPV6互联网IP 地址租用服务 |
| 网站域名备案服务 | 配合使用单位完成网站域名备案 |
| 可操作性 | 支持通过云管理平台，实现申请部署与使用 |

**2、主机负载均衡服务**

|  |  |
| --- | --- |
| 指标项 | 服务要求 |
| 服务能力 | 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 |
| 均衡策略 | 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 |
| 健康检查 | 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 |
| 会话（Session）保持 | 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 |
| 高可用性 | 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% |
| 转发规则 | 提供多种转发规则，满足不同业务场景的要求 |
| 扩展性 | 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 |
| 可操作性 | 支持通过云管理平台，实现申请部署与使用 |
| 协议支持 | 提供 4 层（TCP 协议）和 7 层（HTTP 和 HTTPS 协议）的负载均衡服务 |

**3、远程接入服务**

|  |  |
| --- | --- |
| 指标项 | 服务要求 |
| 功能要求 | 提供堡垒机远程接入服务 |
| 运维审计 | 字符操作审计、图形操作审计、文件操作审计 |
| 访问控制 | 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、SSL VPN接入**

|  |  |
| --- | --- |
| 指标项 | 服务要求 |
| 接入方式 | 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 |
| 身份管理 | 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 |
| 访问控制策略 | 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 |
| 密码要求 | 采用通过商用密码产品认证的SSL VPN产品 |

**5、IPSec VPN接入**

|  |  |
| --- | --- |
| 指标项 | 服务要求 |
| 配置方式 | 通过手工配置或自动配置的方式实现IPSecVPN隧道的建立，支持对IKE策略、IPSec策略配置及对VPN服务、IPSec站点连接的申请并提供状态监控，记录完整的用户访问日志 |
| 基本功能 | 实现IPsec抗重放检测功能、反向路由注入功能，支持IPv6协议 |
| 密码要求 | 采用通过商用密码产品认证的IPSEC VPN产品 |

**6、web应用防火墙防护**

|  |  |
| --- | --- |
| 指标项 | 服务要求 |
| 检测算法 | 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 |
| 部署方式 | 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 |
| 黑名单 | 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 |
| 可操作性 | 支持通过云管理平台，实现申请部署与使用 |

2.2.4云主机深度监控服务

|  |  |
| --- | --- |
| 指标项 | 服务要求 |
| 云主机深度监控 | 提供云主机7\*24小时深度监控服务 |
| 集中告警监控 | 支持多维度告警/事件展现 |
| Top性能监控 | 提供常用指标的TopN性能视图，包括：  服务器、虚拟机的CPU、内存TopN视图；  网络接口流量；  存储读写带宽、读写IOPS、读写IO大小。 |
| 安全事件服务 | 提供主机安全事件的验证、分析，并提供事件报告 |
| 应急处置服务 | 提供特定云主机的应急问题协助排查，协助处理应用故障等服务，并提供相应报告 |
| 值守保障服务 | 提供7x24小时的运维值守工作，不仅限于机房巡检、云平台和硬件监控，同时提供问题排查协助、协助处理应用故障等服务，并提供相应报告 |

2.2.5安全管理服务

投标人所投云平台应具备完备的安全防护体系和安全防护设备，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/T 22239-2019）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；积极配合采购人开展各项安全服务保障工作。投标人管辖范围内的硬件、软件及支撑环境资源，至少达到业务系统的最高安全等级要求。

投标人所投云平台通过中央网信办云计算服务安全评估，提供相关证明并加盖投标人公章。

投标人所投云平台需通过等保三级评估，提供相关证明并加盖投标人公章。

投标人所投云平台应具备商用密码服务能力，并通过商用密码应用安全性评估，提供相关证明并加盖投标人公章。

2.2.6运维服务

**1、服务要求**

投标人需编制服务制度、规范、流程，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。

投标人负责设立技术支持热线，并安排专人值守，为云服务工作提供7\*24小时热线支持服务。投标人针对采购人要求的云平台服务相关内容，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、管理能力要求**

投标人应采用监控软件，提升管理能力，须具有的管理能力要求如下：

（1）后台任务性能分析能力：能够对后台任务慢追踪，包括时间、后台任务名称、平均响应时间；提供后台任务性能分析能力截图。

（2）同时间轴数据分析能力；能够对用户体验层、应用程序层、IT架构层进行同时间轴分析，找到引起业务总分降低的关键指标；提供同时间轴数据分析能力截图。

（3）具有数据库知识库，实现智能诊断分析功能：当某个场景告警时，可以通过知识图谱推荐的诊断路径进行自动化分析，并输出诊断报告；提供智能诊断分析功能和诊断分析报告能力截图。

（4）具有数据库健康模型和性能模型：通过模型，可以随时了解数据库的运行状态和系统的当前负载及性能情况；提供健康模型和性能模型能力截图。

**3、响应的及时性要求**

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，投标人应在5分钟内响应，在30分钟之内开始处理故障，能够协调人力资源在1小时内到达现场提供服务。系统发生宕机问题时，投标人应在30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。

**4、重点保障要求**

为保障春节、五一、十一、两会等重要时期以及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，加大云服务保障力度，保证在业务高峰期内系统平稳运行。

**5、应急保障和风险防控措施**

云平台应具备相应的应急预案与风险防控措施,在云平台运行维护期间，出现应急情况和风险状况时，按照预案处置,快速解决问题。

2.2.7业务连续性保障服务

由于采购人业务系统均属于生产系统，保障业务系统运行的连续性是关键。投标人需具备类似项目经验，可根据业务特点制定应用系统迁移部署方案，配合采购人完成系统迁移部署、运行和安全保障，最终保证现有业务系统可平滑迁移至成交人云平台。具体要求如下：

1）根据采购人需求，完成应用系统的迁移部署。投标人需对迁移过程中是否造成业务中断以及业务中断时间进行承诺。

承诺迁移过程中业务不中断的；

承诺迁移业务中断时间少于10小时；

承诺迁移业务中断时间大于10小时（不包含10小时）但不多于72小时（包含72小时）；

承诺迁移业务中断时间超过72小时（不包含72小时）。

2）根据采购人关键业务系统的异构部署（不同云服务商之间）需求，投标人须配合采购人开展方案设计、实施调试等工作。相关工作不得收取额外费用。投标人需承诺：本项要求下相关工作产生的费用应包含在投标报价中不额外收取费用。

3）由于采购人业务系统主机已部署于北京市政务云平台中，本项目采购结束后可能会涉及部分云主机的跨云迁移工作。对此，投标人需承诺成交后配合采购人积极与原有云平台厂商对接，平滑稳定完成跨云迁移工作。跨云迁移不得额外收取采购人费用。本项目中涉及跨云迁移的工作，应该在本项目签订合同之日起1个月内完成。投标人需承诺：如因投标人一方政务云环境未能满足迁移要求，造成采购人无法在合同签订之日起1个月内完成跨云迁移工作的，自第2个月起，成交人应承担采购人在原有服务商云环境中相关主机的一切租用服务费用，直至相关系统完成迁移工作为止。

**投标人针对以上1-3项内容提供迁移承诺书并加盖投标人公章。**

2.3运维团队要求

投标人须根据项目要求安排具备相应资质和经验的专业人员从事本项目工作，提供不少于10人的服务团队，须确保项目实施队伍的稳定。投标人需提供项目团队组织架构、成员名单、成员职责，保证担任重要岗位的人员具备相应专业资质。

**（1）项目经理**

项目经理1名，需具有5年及以上项目管理工作经验（提供个人简历、项目经历），需具备有效期内的高级信息系统项目管理师证书（计算机技术与软件专业技术资格）、信息安全保障人员认证证书（应急服务专业级或以上）、信息安全保障人员认证证书（安全运维专业级或以上）、信息技术应用创新考试评价证书（信创集成项目管理师）、信息技术应用创新考试评价证书（系统架构师）、重要信息系统安全等级保护认证证书等。

**（2）安全（技术）负责人**

安全（技术）负责人员1名（不能与项目经理为同一人），需具有五年以上工作经验，需具有在有效期内的信息安全保障人员认证证书（安全集成专业级或以上）、信息安全保障人员认证证书（应急服务专业级或以上）、注册信息安全工程师（CISP）认证证书等。

**（3）团队人员**

其他团队服务人员不少于8名（不包含项目经理和安全技术负责人），团队人员需具备以下技术资格认定证书：系统架构设计师证书、系统分析师证书、信息系统项目管理师证书、系统规划与管理师证书、网络规划设计师证书、数据库系统工程师证书、注册信息安全工程师（CISP）认证证书。

## **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。

4.2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。