**采购需求**

**一、采购标的**

1. 采购标的

|  |  |  |
| --- | --- | --- |
| 标的名称 | 采购包预算金额  （万元） | 数量 |
| 北京市政法办案智能管理系统政务  云租用项目 | 482.13538 | 1 |

2. 项目背景/项目概述

本项目以租用北京市级政务云平台资源的方式部署北京市政法办案智能管理系统，通过租用北京市级政务云平台上的计算资源、存储资源、网络资源和安全服务资源，根据业务应用系统需求对其进行集成、整合，联通公检法司等具有政法办案职能的政法业务系统，为本项目的业务应用系统提供安全、可靠、稳定的系统部署环境。此外业务系统在入云后还需重新备案并开展信息系统安全等级保护三级测评工作，并持续做好系统建设和运行期间的安全防护。现有信息系统情况如下：

1. BJCM-外网中心平台

该系统于2017年8月正式启动建设工作；2019年1月全面进入施工阶段；2019年5月开始局部试点；2019年9月起在全市118家履行刑事办案职能的政法单位全面试点；2022年4月底完全项目竣工验收。

BJCM-外网中心平台包含刑事诉讼协同办案子系统、电子卷宗智能化、量刑辅助、知识索引和类案推送、录音录像智能审查、证据审查校验、远程智能庭审、文书智能校验、智能消息提醒、执法监督智能案件评查、刑事案件智能繁简分流、案件智能态势分析、涉案财物智能分析、卷宗巡查系统等十几个业务系统

1. BJCM-综治管理平台

BJCM-系统综治管理平台由7个子系统（2个电子政务内网、5个电子政务外网），其中平安北京建设考核系统和重点地区整治工作系统依托电子政务内网建设，综治中心工作系统、群防群治工作系统、外网日常办公系统、政务外网门户系统和城乡结合部整治工作系统依托政务外网建设。本期采购资源将支撑政务外网的5个系统。

**二、商务要求**

**（一）服务地点**

由采购人指定。

**（二）服务期限**

2025年7月-2026年7月

**（三）支付方式**

本项目采用分期付款的方式，双方签订合同后且财政资金到位，且采购人完成经费审核程序后30个工作日内支付合同总价款的50%;租用期满且财政资金到位后，采购人在完成经费审核程序后向中标人付清余款，余款金额为本合同总价款50%。支付方式详见合同。

**（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

（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。

**三、技术要求**

1. **政务云基础服务技术参数要求**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **编号** | **服务类别** | **服务子类** | **服务项** | **计价单位** | **本项目需求** |
| 1 | 计算服务 | x86平台云主机服务 | vCPU（主频不低于2.4GHz） | 1CPU | 582 |
| 2 | 内存 | 1GB | 2068 |
| 3 | x86物理服务器租用服务 | x86物理服务器配置1：2路12核，主频≧2.0GHz，64G内存，2块600G SAS硬盘，2个HBA卡，2个万兆端口 | 1台 | 1 |
| 4 | x86物理服务器配置3：8路16核主频≧2.0GHz，256G内存，2块600G SAS硬盘，2个HBA卡，2个万兆端口 | 1台 | 15 |
| 5 | 存储服务 | 普通存储 | 普通存储（单盘技术指标: 单盘 IOPS 2000-5000 ） | 1 Gb | 60397 |
| 6 | 高性能存储 | 高性能存储（单盘技术指标：单盘 IOPS 10000-25000 ） | 1 Gb | 67000 |
| 7 | 本地备份服务 | 本地备份服务 | GB | 14500 |
| 8 | 网络服务 | 远程接入服务 | 远程接入运维 | 1账号 | 3 |
| 9 | VPN服务 | SSL VPN 接入 | 1套 | 3 |
| IPSec VPN接入 | 1Mb带宽 | 1000 |
| 10 | 云主机深度监控服务 | 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（500核CPU,1824G内存） | 1主机 | 59 |

**（二）政务云扩展服务技术参数要求**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **服务类别** | **服务子类** | **服务项** | **计价单位** | **本项目需求** |
| 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，根据漏洞扫描结果或等级测试要求对操作系统进行安全加固。 | 1个云主机 | 7 |
| 国产Linux套餐：国产Linux操作系统服务租用、安装及维护，根据漏洞扫描结果或等级测试要求对操作系统进行安全加固。 | 1个云主机 | 52 |
| 安全服务 | 主机杀毒服务 | 主机杀毒服务 | 1台 | 59 |
| 主机防护 | 主机防护 | 1台 | 59 |
| 主机安全加固 | 主机安全加固 | 1台 | 59 |
| 网页防篡改服务 | 网页防篡改服务 | 1监控点 | 3 |
| 安全检测监测、审计服务 | 主机漏洞扫描 | 主机漏洞扫描 | 1台（4次） | 59 |
| 数据库审计服务 | 数据库审计服务 | 1套 | 4 |
| 定制化服务 | 渗透测试服务 | 渗透测试服务（不少于2次） | 1套 | 2 |
| 脆弱性检查服务 | 脆弱性检查服务 | 1套 | 2 |
| 等保测评服务 | 等保测评服务（三级） | 1套 | 2 |
| 应急演练 | 应急演练（不少于2次） | 1套 | 2 |

**四、采购目标**

本项目的总体目标是通过租用政务云平台基础和扩展服务，对“北京市政法办案智能管理系统”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. 提供政务云扩展服务，包括基础软件支撑服务、安全服务、安全检测监测、审计服务和个性化等服务。
3. 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。
4. 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。

**五、服务内容与服务标准**

**（一）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； |

1. **存储服务**

**2.1普通性能存储**

|  |  |
| --- | --- |
| **指标项** | **规格要求** |
| 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 |

**2.2高性能存储**

|  |  |
| --- | --- |
| **指标项** | **规格要求** |
| 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 |

**2.3备份服务**

通过备份策略实现对用户数据（文件、操作系统、数据库）的本地备份和异地备份（不包含备份存储空间费用），默认提供非结构化数据保护、Windows/Linux操作系统备份保护及对应平台的数据库、文件备份保护。备份服务应满足如下要求:

（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。

云服务商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。

**（三）网络服务**

**3.1远程接入服务**

|  |  |
| --- | --- |
| **指标项** | **规格要求** |
| 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； |

**3.2 SSL VPN服务**

|  |  |
| --- | --- |
| **指标项** | **规格要求** |
| 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 |

**（四）云主机深度监控服务**

|  |  |
| --- | --- |
| **指标项** | **规格要求** |
| 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 |

**（五）基础软件支撑服务**

5.1商业操作系统套餐

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。

**（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。安全服务主要内容包含：

6.1.1 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。

6.1.2 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。

6.1.3 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。

6.1.4 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。

**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，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。

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，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。

6.2.3 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。

6.2.4 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；通过商用密码应用安全性评估；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；

**（七）运维服务**

**7.1服务内容**

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。

**7.2服务标准**

7.2.1 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2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。

7.2.2 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。

7.2.3 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。

7.2.4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。

7.2.5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。

7.2.6运维管理能力要求

投标人应采用运维监控软件，提升运维管理能力，须具有的运维管理能力要求如下：

（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）具有数据库运维知识库，实现智能诊断分析功能：当某个运维场景告警时，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。

**（八）迁移服务**

**8.1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。

**8.2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：

8.2.1 投标人需编制业务连续性服务方案。

8.2.2 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，进行风险评估，提出详细解决方案。

8.2.3 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。

8.2.4 本项目如涉及系统迁移，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5个工作日内完成跨云迁移工作的，自第6个工作日起，中标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。

**（九）培训服务**

投标人提供云服务操作手册，并为采购人提供必要的使用培训，至少提供以下内容：

9.1 面向项目管理人员、系统管理人员的培训，确保此类人员能清晰地了解云平台的设计理念和设计方法，掌握云平台的整体结构，以及各类云资源的申请、审核、开通、回收等管理流程。

9.2 面向系统维护人员的培训，确保此类人员能理解和掌握云平台的相关技术知识，能够熟练地维护云平台，快速定位和解决系统出现的问题，保证云平台服务期间正常运转，并持续提高运维服务质量。

**（十）其他服务**

按照采购人的有关管理规定及具体需求提供定制化服务，包括渗透测试服务、脆弱性检查服务、等保测评服务、应急演练服务。

**六、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名技术经理及5名以上项目团队专职人员，为本项目提供服务。驻场项目经理需按照采购人要求，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） 4. 重要信息系统安全等级保护培训证书（CIIP） |
| 技术经理 | 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（CISE）认证证书 |
| 项目  人员 | 5 | 专科及以上 | 有3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、CISP证书 |

**七、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。

**八、其他相关要求**

**（一）行业特定资格要求**

根据工业和信息化部《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号文件，投标人应取得互联网资源协作服务业务许可：

1.投标人须提供《中华人民共和国增值电信业务经营许可证》复印件：

（1）该许可证中的业务种类包含“第一类增值电信业务中的互联网数据中心业务”及业务覆盖范围包含北京；如有“不含互联网资源协作服务的机房所在地”描述的，须不包含北京；

（2）该许可证中的业务种类包含“第一类增值电信业务中的互联网数据中心业务”且业务覆盖范围（服务项目）为包含北京在内的互联网资源协作服务。

投标人提供的《中华人民共和国增值电信业务经营许可证》复印件中的表述内容符合上述两种情形任何一种的均合格。

2.如投标人无法提供符合上述情形的《中华人民共和国增值电信业务经营许可证》复印件的，投标人应如实提供相关说明及行业主管部门出具的证明材料，证明其已取得互联网资源协作服务业务许可且业务覆盖范围包含北京。投标人不提供真实情况的，情节严重的将根据政府采购相关法律法规追究法律责任。

**（二）供应商评审项证书**

|  |  |
| --- | --- |
| 序号 | 证书或测评名称 |
| 1 | 投标人承建及运营的政务云平台，至少有一项在其上运行的信息系统应按照《信息安全技术网络安全等级保护基本要求》（GB/T22239-2019）第三级要求，完成等保三级的测评，得分不低于（70）分且无高风险问题 |
| 2 | 投标人承建及运营的政务云平台，至少有一项在其上运行的信息系统通过中共中央网络安全和信息化委员会办公室/国家互联网信息办公室云计算服务安全评估 |
| 3 | 投标人承建及运营的政务云平台，至少有一项在其上运行的信息系统应按照《信息安全技术信息系统密码应用基本要求》（GB/T 39786-2021）第三级要求，完成商用密码应用安全性评估，评估得分不低于（60）分且系统无高风险项 |
| 4 | 质量管理体系认证证书 |
| 5 | 信息安全管理体系认证证书 |
| 6 | 信息技术服务管理体系认证证书 |

**（三）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。