**第四章 采购需求**

## 第01包：机关政务外网云基础服务

# 一、采购标的

# 1.采购标的

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 服务子类 | 服务项 | 计价单位 | 报价单位 | 数量 | 期限（月） |
| x86平台云主机服务 | vCPU（主频不低于2.4GHz） | 1CPU | 元/月 | 932 | 12 |
| 内存 | 1GB | 元/月 | 1792 | 12 |
| 图形图像计算服务 | GPU显存不低于12G，最大单精度浮点计算能力不低于5TFLOPS | 1GPU | 元/月 | 48 | 12 |
| 高性能存储 | 高性能存储（单盘技术指标：单盘IOPS 3000-20000 ） | 1GB | 元/月 | 56680 | 12 |
| 本地备份 | 普通性能存储（单盘技术指标: 单盘IOPS 1000-3000 ） | 1GB | 元/月 | 56680 | 12 |
| 本地备份服务 | 1GB | 元/月 | 56680 | 12 |
| 互联网链路服务 | 互联网链路带宽（共享） | 1Mb | 元/月 | 10 | 12 |
| 互联网IP地址租用服务、并提供备案服务 | 1IP | 元/月 | 5 | 12 |
| 远程接入服务 | 远程接入服务 | 1账号 | 元/月 | 15 | 12 |
| WAF防护 | 互联网web应用防火墙服务 | 1IP | 元/月 | 5 | 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 | 50 | 12 |

# 2.项目背景或概况

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，北京市人大常委会机关政务外网系统自2018年起迁入市政务云。本项目通过租用政务云平台基础服务，对系统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。

# 二、商务要求

## （一）服务地点

北京市政务云机房

## （二）服务期限

自合同签订之日起12个月

## （三）支付方式

服务费用分三笔支付：

第一笔：双方签订合同且财政资金下达（具体时间以采购人确认的情况为准）后30个工作日内，支付合同总额的40%；

第二笔：2025年9月底前，采购人对项目进行阶段性验收，验收通过后支付合同总额的40%；

第三笔：服务期满，采购人对项目进行竣工验收，验收通过后支付合同总额的20%。

# 三、技术要求

## （一）云主机服务

**1.1服务内容**

按照采购人的具体需求，提供云主机服务，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。

**1.2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 云主机提供基于GPU图形图像计算服务；

1.2.4 应满足云主机之间、CPU之间隔离保护要求；

1.2.5 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；

1.2.6 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；

1.2.7 支持异构虚拟化能力，如KVM等多种虚拟化技术；

1.2.8 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；

1.2.9 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；

1.2.10 云计算资源性能要求包括但不限于如下：

1.2.10.1 云主机CPU主频不低于2.40 GHz；

1.2.10.2 云主机内存硬件配置不低于DDR4-2400MHz；

## （二）存储服务

**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、高性能存储和本地备份服务，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；

2.2.6 存储资源性能要求包括但不限于如下：

2.2.6.1 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。

## （三）网络服务

**3.1服务内容**

3.1.1 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。

3.1.2 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。

3.1.3 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。

**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 网络系统性能要求包括但不限于如下：

3.2.9.1 政务云政务外网出口总带宽10Gbps；

3.2.9.2 政务云互联网出口总带宽5Gbps；

3.2.9.3 云主机云内相互调用带宽不低于1Gb/s；

3.2.9.4 数据传输中的丢包比例低于0.01%。

3.2.10 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；

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。重要保障时期可以做到远程接入账号禁用操作，根据需求随时执行远程接入账号管控操作，并根据需求导出运维录屏操作记录。

## （四）运维服务

**4.1服务内容**

4.1.1 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；

4.1.2 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；

4.1.3 执行云平台变更申请、审批流程；

4.1.4 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；

4.1.5 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。

**4.2服务标准**

4.2.1 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15分钟内响应，能够协调人力资源在2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。

4.2.2 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。

4.2.3 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。

4.2.4 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 。

4.2.5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。

4.2.6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。

4.2.7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异地备份。

4.2.8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。

## （五）备份服务

**5.1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。

**5.2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（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:

5.2.1 备份介质本身具备高可用性和冗余性。

5.2.2 备份方式包括完整备份、差异备份和增量备份。

5.2.3 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。

5.2.4 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。

5.2.5 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。

## **（六）迁移服务**

**6.1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。

**6.2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：

6.2.1 投标人需编制业务连续性服务方案。

6.2.2 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。

6.2.3 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。

## （七）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：

**7.1内部培训**

内部培训旨在提高云平台运维能力，规范运维管理。内容包括但不限于：

7.1.1 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。

7.1.2 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。

7.1.3 本单位人员的安全培训教育，确保工作人员符合岗位要求。

7.1.4 云平台维护人员的定期业务培训和保密培训，重保前的业务培训和应急保障培训等。

7.1.5 面向管理单位的培训，确保此类人员充分了解云平台的技术架构、服务水平等。

**7.2外部培训**

投标人应根据本项目的特点制定培训方案并提供培训，负责安排专业培训讲师授课，并提供全套培训教材和培训课程计划表，培训课程涵盖云平台使用和管理培训，采购人在培训后能够独立使用相关服务功能。投标人每年应组织安排至少一次针对采购人的系统入云及用户培训，培训规模应至少10人次。投标人应将所有培训费用（含培训教材费）及各项支出计入资源租赁费用中，不单独报价。内容包括但不限于：

7.2.1 面向采购人和开发人员的技术交流，包括云架构规划咨询、应用系统部署、迁移，云平台运维及其他技术服务。

7.2.2 面向采购人的培训，确保云平台最终用户能理解和掌握各类云服务的使用方法和操作技巧，能够高效、熟练地基于云平台部署上层业务应用，最终使采购人在培训后能够独立使用相关服务功能，而不必依赖投标人现场指导。

7.2.3 面向开发人员的培训，确保其能理解和掌握基于云平台的开发规范，针对具体的业务应用场景能够充分发挥云平台的技术优势，合理地设计上层业务应用的技术架构，制订部署、迁移方案，评估云资源的容量需求。

7.2.4 定期对系统相关的人员进行应急预案培训，并进行应急预案的演练；每年至少开展1次云平台应急演练。

7.2.5 投标人应在此基础上制定针对本单位的培训方案。

## （八）其他服务

**8.1服务规范**

投标人须严格按照采购人制定的管理办法、流程及其他汇报制度、应急制度、文档管理、资产管理、基线管理、人员管理、培训与考试、知识库管理、安全管理等相关制度，开展标准化运维工作。

投标人应遵从政务云管理单位的日常管理要求，包括但不限于应使用政务云管理单位指定的安全通信工具，确保通信和协调信息处于可控范围。

**8.2支撑保障服务**

按照采购人有关国产数据库改造、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。

**8.4其他技术服务**

投标人可根据采购人具体需求提供性能测试、性能调优、深度巡检、重保护航、全链路压测、专项咨询等服务。

## （九）验收要求

**9.1服务绩效指标**

1. 云服务全年整体可用性≥99.99%；
2. 数据可靠性应不低于 99.9999 %

（3）故障响应率100%；

（4）应急响应时间≤5分钟（云主机停止运行、网络无法连接等重大事件1分钟内响应）；

**9.2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6小时及以上。

（3）服务期满后5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验收评审，方可通过验收。

# 四、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.该项目服务团队要求配备项目经理1人、技术负责人1人以及相应实施人员，项目团队总人数不少于8人（含项目经理和技术负责人）。其中：

项目经理：应5年以上相关工作经验，具有信息系统项目管理师（高级）证书和网络规划设计师（高级）证书，具有优秀的大型项目团队管理能力，善于协调各方资源，保证项目服务期保障要求。

技术负责人：应具有5年以上相关工作经验，具有CISP(注册信息安全工程师)资格证书。

其他项目组成员：不少于6名（不含项目经理和技术负责人），具有5年以上相关工作经验。

项目经理应是专职负责人，在服务期内不可更换。项目成员保证60%以上为固定人员，项目成员如有变化，需提前10个工作日通知采购人，经采购人审批同意后方可更换。

# 五、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。

## 第02包：机关互联网云基础服务

# 一、采购标的

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 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 | x86平台云主机服务 | vCPU（主频不低于2.4GHz） | 1CPU | 元/月 | 228 | 12 |
| 内存 | 1GB | 元/月 | 572 | 12 |
| 存储服务 | 高性能存储 | 高性能存储（单盘技术指标：单盘IOPS 10000-25000 ） | 1GB | 元/月 | 15360 | 12 |
| 网络服务 | 互联网链路服务 | 互联网链路带宽（共享） | 1Mb | 元/月 | 300 | 12 |
| 互联网链路服务 | 互联网IP地址租用服务、并提供备案服务 | 1IP | 元/月 | 5 | 12 |
| 主机负载均衡服务 | 主机负载均衡服务（内网） | 1IP | 元/月 | 6 | 12 |
| 远程接入服务 | 远程接入服务 | 1账号 | 元/月 | 5 | 12 |
| VPN服务 | SSL VPN接入 | 1套 | 元/月 | 5 | 12 |
| WAF防护 | 互联网web应用防火墙服务 | 1IP | 元/月 | 5 | 12 |
| 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 | 1主机 | 元/月 | 33 | 12 |

# 2.项目背景或概况

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，北京市人大常委会机关互联网系统自2018年起迁入市政务云。本项目通过租用政务云平台基础服务，对系统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。

# 二、商务要求

## （一）服务地点

北京市政务云机房

## （二）服务期限

自合同签订之日起12个月

## （三）支付方式

服务费用分三笔支付：

第一笔：双方签订合同且财政资金下达（具体时间以采购人确认的情况为准）后30个工作日内，支付合同总额的40%；

第二笔：2025年9月底前，采购人对项目进行阶段性验收，验收通过后支付合同总额的40%；

第三笔：服务期满，采购人对项目进行竣工验收，验收通过后支付合同总额的20%。

# 三、技术要求

## （一）云主机服务

**1.1服务内容**

按照采购人的具体需求，提供云主机服务，包括：x86平台云主机服务和x86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。

**1.2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 云计算资源性能要求包括但不限于如下：

1.2.9.1 云主机CPU主频应不低于2.4GHz；

## （二）存储服务

**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、静态存储和本地备份服务，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；

2.2.6 存储资源性能要求包括但不限于如下：

2.2.6.1 高性能单盘技术指标满足IOPS 10000-25000；

## （三）网络服务

**3.1服务内容**

3.1.1 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。

3.1.2 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。

3.1.3 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。

3.1.4 VPN服务，含SSL VPN接入与IPSec VPN接入服务。

**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 网络系统性能要求包括但不限于如下：

3.2.9.1 云内骨干线路带宽不低于10Gb/s；

3.2.9.2 服务器业务带宽不低于20Gb/s；

3.2.10 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；

3.2.11 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。

3.2.12 IPSec VPN接入须可采用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，能够记录完整的用户访问日志；实现IPsec抗重放检测功能、反向路由注入功能，支持IPv6协议；采用通过商用密码产品认证的IPSEC VPN产品。

3.2.13 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。

## （四）运维服务

**4.1服务内容**

4.1.1 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；

4.1.2 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；

4.1.3 执行云平台变更申请、审批流程；

4.1.4 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；

4.1.5 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。

**4.2服务标准**

4.2.1 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30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。

4.2.2 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。

4.2.3 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。

4.2.4 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 。

4.2.5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。

4.2.6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。

4.2.7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异地备份。

4.2.8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。

## （五）备份服务

**5.1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。

**5.2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（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:

5.2.1 备份介质本身具备高可用性和冗余性。

5.2.2 备份方式包括完整备份、差异备份和增量备份。

5.2.3 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。

5.2.4 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。

5.2.5 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。

## （六）日志服务

**6.1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：

6.1.1 提供统一收集PaaS平台组件的日志服务；

6.1.2 提供收集面向应用的日志服务，如应用定向写到文件中的日志；

6.1.3 提供对日志的可视化管理、组合过滤查询的能力；

6.1.4 支持用户自定义解析规则和解析规则组，并预制多种解析规则实现日志数据解析；

6.1.5 日志数据冷热数据分离存储，支持分别配置冷数据和热数据保存时间，也可支持永久保存；

6.1.6 支持自定义日志分片数和副本数；

6.1.7 为了提高存储资源利用率，支持日志投递功能，按JSON、CSV等转存格式转储日志数据到共享存储。

**6.2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。

## （七）迁移服务

**7.1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。

**7.2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：

7.2.1 投标人需编制业务连续性服务方案。

7.2.2 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。

7.2.3 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1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。

## （八）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：

**8.1内部培训**

内部培训旨在提高云平台运维能力，规范运维管理。内容包括但不限于：

8.1.1 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。

8.1.2 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。

8.1.3 本单位人员的安全培训教育，确保工作人员符合岗位要求。

8.1.4 云平台维护人员的定期业务培训和保密培训，重保前的业务培训和应急保障培训等。

8.1.5 面向管理单位的培训，确保此类人员充分了解云平台的技术架构、服务水平等。

**8.2外部培训**

投标人应根据本项目的特点制定培训方案并提供培训，负责安排专业培训讲师授课，并提供全套培训教材和培训课程计划表，培训课程涵盖云平台使用和管理培训，采购人在培训后能够独立使用相关服务功能。投标人每年应组织安排至少一次针对采购人的系统入云及用户培训。投标人应将所有培训费用（含培训教材费）及各项支出计入资源租赁费用中，不单独报价。内容包括但不限于：

8.2.1 面向采购人和开发人员的技术交流，包括云架构规划咨询、应用系统部署、迁移，云平台运维及其他技术服务。

8.2.2 面向采购人的培训，确保云平台最终用户能理解和掌握各类云服务的使用方法和操作技巧，能够高效、熟练地基于云平台部署上层业务应用，最终使采购人在培训后能够独立使用相关服务功能，而不必依赖投标人现场指导。

8.2.3 面向开发人员的培训，确保其能理解和掌握基于云平台的开发规范，针对具体的业务应用场景能够充分发挥云平台的技术优势，合理地设计上层业务应用的技术架构，制订部署、迁移方案，评估云资源的容量需求。

8.2.4 定期对系统相关的人员进行应急预案培训，并进行应急预案的演练；每年至少开展1次云平台应急演练。

8.2.5 投标人应在此基础上制定针对本单位的培训方案。

## （九）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，包括数据库租用服务、数据库安全加固服务、网站安全管理服务、安全隔离网闸租赁服务、网站监测服务-网站页面访问性能监控、等保测评、业务拓展保障服务。

**9.1服务规范**

投标人须严格按照采购人制定的管理办法、流程及其他汇报制度、应急制度、文档管理、资产管理、基线管理、人员管理、培训与考试、知识库管理、安全管理等相关制度，开展标准化运维工作。

投标人应遵从政务云管理单位的日常管理要求，包括但不限于应使用政务云管理单位指定的安全通信工具，确保通信和协调信息处于可控范围。

**9.2支撑保障服务**

按照采购人有关国产数据库改造、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。

**9.3其他技术服务**

提供性能测试、性能调优、深度巡检、重保护航、全链路压测、专项咨询等服务。

## （十）验收要求

**10.1服务绩效指标**

1. 云服务全年整体可用性≥99.99%；
2. 数据可靠性应不低于 99.9999 %

（3）故障响应率100%；

（4）应急响应时间≤5分钟（云主机停止运行、网络无法连接等重大事件1分钟内响应）；

**10.2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2小时及以上。

（3）服务期满后5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验收评审，方可通过验收。

# 四、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。

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（安全运维专业级或以上、信息安全保障人员认证证书（应急服务专业级或以上）、重要信息系统安全等级保护培训证书（CIIP）等。

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（CISE）认证证书等。

其他项目团队成员：不少于8名（不包含项目经理和安全（技术）负责人），团队人员须具备以下证书：系统规划与管理师资质证书（高级）、系统分析师资质证书（高级）、系统架构设计师认证证书（高级）、CISP证书。

# 五、 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。