1. **采购需求**

政务云服务第1包

1. **采购标的**

1. 采购标的

（1）北京市免疫规划信息管理系统

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 序号 | 分项名称 | | | | 数量 |
| 服务类别 | 服务子类 | 服务项 | 计价单位 |
| 1 | 计算服务 | x86平台云主机服务 | vCPU（主频不低于2.4GHz） | 1 CPU | 622 |
| 2 | 内存 | 1 GB | 2674 |
| 3 | x86物理服务器租用服务 | x86物理服务器配置2：4路10核2.0Ghz，128G内存，2块600G SAS硬盘，2个HBA卡，2个万兆端口 | 1 台 | 4 |
| 4 | 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 | 41650 |
| 5 | 高性能存储 | 高性能存储（单盘技术指标：单盘IOPS 3000-20000 ） | 1 GB | 18920 |
| 6 | 本地备份服务 | 本地备份服务 | 1GB | 10600 |
| 7 | 异地备份服务 | 异地备份服务 | 1GB | 9850 |
| 8 | 网络服务 | 互联网链路服务 | 互联网链路带宽 | 1 Mb | 100 |
| 9 | 互联网IP地址租用服务、并提供备案服务 | 1 IP | 7 |
| 10 | 主机负载均衡服务 | 主机负载均衡服务 | 1 IP（内网） | 2 |
| 11 | 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 | 7 |
| 12 | VPN服务 | SSL VPN接入，用户通过SSL VPN访问业务系统。每套10个并发用户。所需带宽参照“互联网链路带宽”购买。 | 1套 | 100 |
| 13 | 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） | 7 |
| 14 | 其他服务 | 中标麒麟高级服务器版LINUX6.0 | 中标麒麟高级服务器操作系统软件V6.0 Linux 租用服务（提供正版安装介质及授权）。28套信息系统应用服务器所需（按12个月计算），8套信息系统等保测评所需（按3个月计算）。 | 1套 | 72 |
| 15 | WindowsServer标准版2处理器许可及软件保障租用服务 | Windows Server 标准版 2处理器许可及软件保障租用服务（提供正版安装介质及授权）。 | 1套 | 3 |
| 16 | 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 | 76 |
| 17 | 网络防篡改服务 | 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，做到静态页面的实时同步，减少用户页面被恶意篡改的可能性。对业务系统互联网接入系统、APP接入（专业、公众）系统等对外服务应用提供网页防篡改服务 | 1台 | 8 |
| 18 | 主机漏洞扫描 | 用于提供针对主机层面的安全扫描服务，并反馈相关结果。48台生产主机和4台物理服务器，每台主机每年扫描2次。其他24台主机每年每台扫描1次 | 1台 | 128 |
| 19 | 商用中间件租用服务 | 提供商用中间件租用服务（提供正版安装介质及授权），12套应用服务器所需 | 1套 | 12 |
| 20 | 商用数据库（包含RAC组件） | 提供商用数据库（包含RAC组件）租用服务（提供正版安装介质及授权） | 1套 | 4 |
| 21 | 数字签名验签服务器设备租用服务 | 对外提供基于数字证书的身份认证服务、数据签名与签名验证服务、加解密服务和数字信封服务；支持Windows、Linux、AIX等主流应用平台；支持Java、COM、C等应用集成接口；支持RSA、SM2等签名算法。硬件规格：2U；2个100/1000M自适应网口；双电源。主要性能参数：RSA签名4500次/秒，SM2签名4000次/秒。（分别部署在互联网区和政务外网区，互联网区为互联网接入的学校查验证业务和接种单位用户提供CA数字证书认证；政务外网区为经政务外网接入的接种单位终端提供CA数字证书认证。） | 1台 | 2 |

1. 北京市新冠疫苗接种管理平台

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 序号 | 分项名称 | | | | 数量 |
| 服务类别 | 服务子类 | 服务项 | 计价单位 |
| 1 | 计算服务 | x86平台云主机服务 | vCPU（主频不低于2.4GHz） | 1 CPU | 1822 |
| 2 | 内存 | 1 GB | 8344 |
| 3 | x86物理服务器租用服务 | x86物理服务器配置1：2路10核2.0Ghz，64G内存，2块600G SAS硬盘,2个HBA卡，2个万兆端口 | 1 台 | 6 |
| 4 | x86物理服务器配置2：4路10核2.0Ghz，128G内存，2块600G SAS硬盘，2个HBA卡，2个万兆端口 | 1 台 | 6 |
| 6 | 内存-32GB内存 | 1条 | 144 |
| 7 | 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 | 84512 |
| 8 | 高性能存储 | 高性能存储（单盘技术指标：单盘IOPS 3000-20000 ） | 1 GB | 84512 |
| 9 | 本地备份服务 | 本地备份服务 | 1GB | 84512 |
| 10 | 网络服务 | 互联网链路服务 | 互联网链路带宽 | 1 Mb | 50 |
| 11 | 互联网IP地址租用服务、并提供备案服务 | 1 IP | 4 |
| 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 | 30 |
| 13 | VPN服务 | SSL VPN接入，用户通过SSL VPN访问业务系统。每套10个并发用户。所需带宽参照“互联网链路带宽”购买。 | 1套 | 450 |
| 14 | 其他服务 | 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 | 180 |
| 15 | 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 | 180 |

1. 北京市传染病智慧化多点监测触发预警平台（基础）

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 序号 | 分项名称 | | | | 数量 |
| 服务类别 | 服务子类 | 服务项 | 计价单位 |
| 1 | 计算服务 | x86平台云主机服务 | vCPU（主频不低于2.4GHz） | 1 CPU | 774 |
| 2 | 内存 | 1 GB | 2326 |
| 3 | 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 | 129520 |
| 4 | 高性能存储 | 高性能存储（单盘技术指标：单盘IOPS 3000-20000 ） | 1 GB | 64760 |
| 5 | 本地备份服务 | 本地备份服务 | 1GB | 64760 |
| 6 | 异地备份服务 | 异地备份服务 | 1GB | 64760 |
| 7 | 网络服务 | 互联网链路服务 | 互联网链路带宽 | 1 Mb | 200 |
| 8 | 互联网IP地址租用服务、并提供备案服务 | 1 IP | 2 |
| 9 | 主机负载均衡服务 | 主机负载均衡服务 | 1 IP（内网） | 20 |
| 10 | 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 | 10 |
| 11 | 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） | 2 |

1. 北京市卫生防病监测信息资源整合分析平台

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 服务类别 | 服务项 | 服务数量 | 计价单位 | 报价单位 |
| 计算服务 | vCPU(主频不低于2.4GHz) | 89 | 1CPU | 元/月 |
| 内存 | 308 | 1GB | 元/月 |
| x86物理服务器配置1:2路10核2.0Ghz,64G 内存，2块600GSAS硬盘，2个HBA卡，2个万 兆端口 | 2 | 1台 | 元/月 |
| 存储服务 | 普通存储(单盘技术指标：单盘IOPS1000-3000) | 6120 | 1GB | 元/月 |
| 高性能存储(单盘技术指标：单盘IOPS3000-20000) | 3060 | 1GB | 元/月 |
| 本地备份服务 | 3060 | 1GB | 元/月 |
| 异地备份服务 | 3060 | 1GB | 元/月 |
| 网络服务 | 远程接入服务 | 1 | 1账号 | 元/月 |
| VPN服务 | 450 | 1 套 | 元/月 |
| WAF防护服务 | 1 | 1IP(互联网) | 元/月 |
| 其他服务 | 商用操作系统（windows） | 4 | 1套 | 元/月 |
| 国产商用操作系统(linux) | 3 | 1套 | 元/月 |
| 商用应用中间件套餐 | 2 | 1套 | 元/月 |
| 商用数据库租用 | 1 | 1套 | 元/月 |
| 商用数据库租用（包含RAC组件） | 1 | 1套 | 元/月 |
| 云端抗DDOS服务 | 1 | 1站点 | 元/月 |
| 主机杀毒服务 | 7 | 1 台 | 元/月 |
| 主机防护 | 7 | 1 台 | 元/月 |
| 主机安全加固 | 28 | 1 台 | 元/次 |
| 主机漏洞扫描 | 28 | 1 台 | 元/次 |
| 主机日志分析 | 28 | 1 台 | 元/月 |
| 数据库审计服务 | 3 | 1 套 | 元/月 |
| CDN服务 | 42 | 1 GB | 元/月 |

1. 北京市肠道门诊早期监测预警系统

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 服务类别 | 服务项 | 服务数量 | 计价单位 | 报价单位 |
| 计算服务 | vCPU(主频不低 于2.4GHz) | 49 | 1CPU | 元/月 |
| 内存 | 164 | 1GB | 元/月 |
| 存储服务 | 普通存储(单盘技术指标：单盘IOPS1000-3000) | 4320 | 1GB | 元/月 |
| 高性能存储(单盘技术指标：单盘IOPS3000-20000) | 2160 | 1GB | 元/月 |
| 本地备份服务 | 2160 | 1GB | 元/月 |
| 异地备份服务 | 2160 | 1GB | 元/月 |
| 网络服务 | 远程接入服务 | 1 | 1账号 | 元/月 |
| WAF防护服务 | 1 | 1IP(互联网) | 元/月 |
| 其他服务 | 商用操作系统（windows） | 2 | 1套 | 元/月 |
| 国产商用操作系统(linux) | 1 | 1套 | 元/月 |
| 商用应用中间件套餐 | 1 | 1套 | 元/月 |
| 商用数据库租用 | 1 | 1套 | 元/月 |
| 商用数据库租用（包含RAC组件） | 1 | 1套 | 元/月 |
| 云端抗DDOS服 务 | 1 | 1站点 | 元/月 |
| 主机杀毒服务 | 3 | 1 台 | 元/月 |
| 主机防护 | 3 | 1 台 | 元/月 |
| 主机安全加固 | 12 | 1 台 | 元/次 |
| 主机漏洞扫描 | 12 | 1 台 | 元/次 |
| 主机日志分析 | 12 | 1 台 | 元/月 |
| 数据库审计服务 | 1 | 1 套 | 元/月 |

1. 北京市症状监测信息管理系统

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 服务类别 | 服务项 | 服务数量 | 计价单位 | 报价单位 |
| 计算服务 | vCPU(主频不低 于2.4GHz) | 27 | 1CPU | 元/月 |
| 内存 | 78 | 1GB | 元/月 |
| 存储服务 | 普通存储(单盘技术指标：单盘IOPS1000-3000) | 2160 | 1GB | 元/月 |
| 高性能存储(单盘技术指标：单盘IOPS3000-20000) | 1080 | 1GB | 元/月 |
| 本地备份服务 | 1080 | 1GB | 元/月 |
| 异地备份服务 | 1080 | 1GB | 元/月 |
| 网络服务 | 远程接入服务 | 1 | 1账号 | 元/月 |
| WAF防护服务 | 1 | 1IP(互联网) | 元/月 |
| 其他服务 | 商用操作系统（windows） | 2 | 1套 | 元/月 |
| 国产商用操作系统(linux) | 1 | 1套 | 元/月 |
| 商用应用中间件套餐 | 1 | 1套 | 元/月 |
| 商用数据库租用 | 1 | 1套 | 元/月 |
| 商用数据库租用（包含RAC组件） | 1 | 1套 | 元/月 |
| 云端抗DDOS服 务 | 1 | 1站点 | 元/月 |
| 主机杀毒服务 | 3 | 1 台 | 元/月 |
| 主机防护 | 3 | 1 台 | 元/月 |
| 主机安全加固 | 12 | 1 台 | 元/次 |
| 主机漏洞扫描 | 12 | 1 台 | 元/次 |
| 主机日志分析 | 12 | 1 台 | 元/月 |
| 数据库审计服务 | 1 | 1 套 | 元/月 |

（7）北京市医院传染病监测预警系统

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 服务类别 | 服务项 | 服务数量 | 计价单位 | 报价单位 |
| 计算服务 | vCPU(主频不低 于2.4GHz) | 8 | 1CPU | 元/月 |
| 内存 | 64 | 1GB | 元/月 |
| 存储服务 | 普通存储(单盘技术指标：单盘IOPS1000-3000) | 3480 | 1GB | 元/月 |
| 高性能存储(单盘技术指标：单盘IOPS3000-20000) | 1740 | 1GB | 元/月 |
| 本地备份服务 | 1740 | 1GB | 元/月 |
| 异地备份服务 | 1740 | 1GB | 元/月 |
| 网络服务 | 远程接入服务 | 1 | 1账号 | 元/月 |
| WAF防护服务 | 1 | 1IP(互联网) | 元/月 |
| 其他服务 | 商用操作系统（windows） | 1 | 1套 | 元/月 |
| 国产商用操作系统(linux) | 1 | 1套 | 元/月 |
| 商用应用中间件套餐 | 1 | 1套 | 元/月 |
| 商用数据库租用 | 1 | 1套 | 元/月 |
| 商用数据库租用（包含RAC组件） |  | 1套 | 元/月 |
| 云端抗DDOS服务 | 1 | 1站点 | 元/月 |
| 主机杀毒服务 | 2 | 1 台 | 元/月 |
| 主机防护 | 2 | 1 台 | 元/月 |
| 主机安全加固 | 8 | 1 台 | 元/次 |
| 主机漏洞扫描 | 8 | 1 台 | 元/次 |
| 主机日志分析 | 8 | 1 台 | 元/月 |
| 数据库审计服务 | 1 | 1 套 | 元/月 |

（8）北京市疾控系统疫苗采购进销存管理信息系统

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 服务类别 | 服务项 | 服务数量 | 计价单位 | 报价单位 |
| 计算服务 | vCPU(主频不低 于2.4GHz) | 133 | 1CPU | 元/月 |
| 内存 | 409 | 1GB | 元/月 |
| x86物理服务器配置2:4路10核2.0Ghz,128G内存，2块600GSAS硬盘，2个HBA卡，2个万 兆端口 | 2 | 1台 | 元/月 |
| 存储服务 | 普通存储(单盘技术指标：单盘IOPS1000-3000) | 13080 | 1GB | 元/月 |
| 高性能存储(单盘技术指标：单盘IOPS3000-20000) | 6540 | 1GB | 元/月 |
| 本地备份服务 | 6540 | 1GB | 元/月 |
| 异地备份服务 | 6540 | 1GB | 元/月 |
| 网络服务 | 互联网链路带宽 | 180 | 1Mb | 元/月 |
| 互联网IP地址租用服务、并提供备案服务 | 6 | 1IP | 元/月 |
| 主机负载均衡服务 | 4 | 1IP( 内 网 ) | 元/月 |
| 远程接入服务 | 1 | 1账号 | 元/月 |
| WAF防护服务 | 1 | 1IP(互联网) | 元/月 |
| 其他服务 | 商用操作系统（windows） | 4 | 1套 | 元/月 |
| 国产商用操作系统(linux) | 3 | 1套 | 元/月 |
| 商用应用中间件套餐 | 2 | 1套 | 元/月 |
| 商用数据库租用 | 2 | 1套 | 元/月 |
| 商用数据库租用（包含RAC组件） | 1 | 1套 | 元/月 |
| 云端抗DDOS服务 | 1 | 1站点 | 元/月 |
| 主机杀毒服务 | 7 | 1 台 | 元/月 |
| 主机防护 | 7 | 1 台 | 元/月 |
| 主机安全加固 | 28 | 1 台 | 元/次 |
| 主机漏洞扫描 | 28 | 1 台 | 元/次 |
| 主机日志分析 | 28 | 1 台 | 元/月 |
| 数据库审计服务 | 2 | 1 套 | 元/月 |
| CDN服务 | 145 | 1 GB | 元/月 |

2. 项目背景

北京市疾病预防控制中心（以下简称“市疾控中心”）是根据国务院关于卫生监督、卫生防病体制改革的总体要求，在北京市卫生防疫站、北京市劳动卫生与职业病防治研究所、北京市健康教育所、北京市性病防治所的基础上组建的市级卫生事业单位，承担着北京市传染性疾病、慢性非传染性疾病、学生常见病、病媒生物传播疾病等预防与控制，突发公共卫生事件应急处置和疫情报告和信息管理，食品卫生、环境卫生、放射卫生和职业卫生等健康危害因素的监测与干预，全市居民的健康教育与健康促进和科研教学等工作。

为实现电子政务集约化建设和管理,充分发挥北京市市级政务云(以下简称政务云)的作用,为政务大数据应用奠定基础,依据《国务院关于促进云计算创新发展培育信息产业新业态的意见》(国发〔2015〕5号)和相关政策法规,按照市领导《关于报审电子政务网络升级改造实施方案的请示》的批复精神，“各部门尽可能上云，特例要报批”的要求，结合实际情况，依照国家及北京市统一协调部署，市疾控中心已将北京市免疫规划信息管理系统、北京市新冠疫苗接种管理平台、北京市疾控中心信息系统和北京市传染病智慧化多点监测触发预警平台等四个系统全部部署在政务云环境，整体运行良好，根据《国家信息化领导小组关于加强信息安全保障工作的意见》（中办发〔2003〕27号）、《国家政务信息化项目建设管理办法》（国办发〔2019〕57号）、《北京市市级政务云管理办法》的相关管理办法和安全服务保障要求，市疾控中心需要为入云后的信息系统租用云上基础资源和扩展资源等服务，确保市疾控中心各项业务顺利开展，提升信息系统安全保障能力。

**二、商务要求**

1 交付（实施）的时间（期限）和地点（范围）

交付（实施）的时间（期限）：7个月

交付（实施）的地点（范围）：政务云机房

2.付款条件（进度和方式）

详见合同。

**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，对入云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。

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

1. 《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）
2. 《国家政务信息化项目建设管理办法》（国办发〔2019〕57号）
3. 《政府采购需求管理办法》(财库〔2021〕22号)
4. 《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）
5. 《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）
6. 《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）
7. 《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）
8. 《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）
9. 《基于云计算的电子政务公共平台顶层设计指南》
10. 《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）
11. 《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）
12. 《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）
13. 《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）
14. 《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）
15. 《北京市政务网络和数据安全管理办法》（京经信发〔2023〕57号）
16. 《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

1. 《国家电子政务外网安全接入平台技术规范》
2. 《信息技术—云计算—云服务质量评价指标》（GB/T 37738-2019）
3. 《信息技术—云计算—云服务计量指标》（GB/T 37735-2019）
4. 《信息技术—云计算—云服务采购指南》（GB/T 37734-2019）
5. 《信息技术—云计算—云存储系统服务接口功能》（GB/T 37732-2019）
6. 《信息技术—云计算—云资源监控通用要求》（GB/T 37736-2019）
7. 《信息技术—云计算—云平台间应用和数据迁移指南》（GB/T 37740-2019）
8. 《信息技术—云计算—云服务交付要求》（GB/T 37741-2019）
9. 《信息系统灾难恢复规范》（GB/T 20988-2007）
10. 《信息安全技术 云计算服务安全能力要求》（GB/T 31168-2014）
11. 《信息安全技术 网络安全等级保护定级指南》（GB/T 22240-2020）
12. 《信息安全技术 网络安全等级保护基本要求》（GB/T 22239-2019）
13. 《信息安全技术 网络安全等级保护测评要求》（GB/T 28448-2019）
14. 《信息安全技术 信息系统密码应用基本要求》（GB/T39786-2021）
15. 《信息安全技术 信息安全风险评估方法》（GB/T 20984-2022）
16. 《信息安全技术 云计算服务安全指南》（GB/T 31167-2014）
17. 《信息安全技术 政府网站云计算服务安全指南》（GB/T 38249—2019）
18. 《信息安全技术 云计算安全参考架构》（GB/T 35279—2017）
19. 《信息安全技术 云计算服务安全能力评估方法》GB/T 34942—2017
20. 《信息安全技术 云计算服务运行监管框架》（GB/T 37972—2019）
21. 《信息技术 云资源监控指标体系》（GB/T 37938-2019）
22. 《电子信息系统机房设计规范》（GB50174-2017）
23. 《数据中心电信基础设施标准》（ANSI/TIA-942）
24. 《综合布线系统工程设计规范》（GB 50311—2016）
25. 《云计算关键领域安全指南V4.0》

1.2.3北京市相关标准

1. 《政务云平台建设技术要求》（DB11/T 2169-2023）
2. 《北京市政务云安全技术规范 IaaS云计算平台分册》
3. 《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》
4. 《北京市政务云安全技术规范 信息安全服务接口分册》

1.2.4其他

1. 《北京市市级行政事业单位云计算服务框架协议采购项目（2023 年度）》征集文件第四部分采购需求中技术要求

**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/货物技术要求

2.1采购标的需满足的服务标准、期限、效率等要求

2.1.1云主机服务

**（1）服务内容**

按照采购人的具体需求，提供主机服务，包括：x86平台云主机和x86物理服务器服务，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。

**（2）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. 支持异构虚拟化能力，如KVM多种虚拟化技术；
6. 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；
7. 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；
8. 云计算资源性能要求包括但不限于如下：

* 物理服务器 CPU 主频应不低于2.40GHz；
* 主机内存硬件配置不低于DDR4-2400MHz；
* 可用性不低于99.99%。

2.1.2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、本地备份服务和异地备份服务，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）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：

* 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。
* 支持高可靠性，可靠性不低于99.9999%；

2.1.3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，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. 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。
4. VPN服务，用户通过SSL VPN访问业务系统。

**（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. 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. 应采用集群部署网络控制，以保障升级时业务不中断；
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；
5. 可支持IPv6地址分配，满足业务系统IPv6要求；
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；
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；
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。
9. 网络系统性能要求包括但不限于如下：

* 云内骨干线路带宽不低于10Gb/s；
* 服务器业务带宽不低于1Gb/s；
* 平均可用性不低于99.9%。

1. 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；
2. 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。

2.1.4基础软件支撑服务

**（1）服务内容**

按照采购人的有关管理规定及具体需求，提供商用操作系统、商用应用中间件、商用数据库等软件支撑服务。

**（2）服务标准**

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、Linux操作系统的各种主流版本，并提供操作系统的安装部署和各种故障处理。

1. 商用应用中间件套餐

提供主流商用中间件服务，并提供中间件的安装部署以及各种故障处理和日常维护。

1. 商用数据库套餐

提供商用数据库服务，提供数据库的安装部署和各种故障处理及日常维护。

2.1.5安全服务

**（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，防止重要或敏感数据泄露或被滥用，并建立应急处置体系。安全服务主要内容包含：

1. 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。

1. 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。

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。

1. 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。

1. 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。

1. 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。

1. 主机漏洞扫描

基于漏洞数据库，通过扫描等手段对主机安全脆弱性进行检测。

**（2）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。
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，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/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；
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。

2.1.6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。

**（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3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. 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 。
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。
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。
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。
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。

2.1.7备份服务

**（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。

**（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:

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。
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。

2.1.8日志服务

**（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：

1. 提供收集面向主机的日志服务；
2. 提供对日志的可视化管理、组合过滤查询的能力；
3. 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。

**（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。

2.1.9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。

**（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：

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。

2.1.10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：

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。
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。
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。
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。
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。

2.2采购标的的其他技术、服务等要求

2.2.1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。

2.2.2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。

3.验收标准

3.1服务绩效指标

3.1.1云服务全年整体可用性≥99.9%；

3.1.2故障响应率100%；

3.1.3应急响应时间≤15分钟；

3.2项目验收要求

采购人在服务期满后 15 个工作日内对投标人服务情况进行验收。投标人应当在验收前向采购人提交验收材料。验收合格的，采购人在验收材料上盖章或签字；验收不合格的，投标人应当在【5】日内进行返工或调整，并重新提交采购人验收。

4.其他要求

4.1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。

4.2投标人须提供1名项目经理及7名项目团队专职人员，为本项目提供服务。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10年及以上类似工作经验 | **可使用证书：**  信息系统项目管理师  注册信息安全工程师证书（CISP）  信息安全保障人员认证证书（CISAW）  网络工程师 |
| 技术负责人 | 1 | 本科及以上 | 有5年及以上类似工作经验 |
| 项目  人员 | 6 | 本科及以上 | 有5年及以上类似工作经验 |

4.3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。

政务云服务第2包

1. **采购标的**

1. 采购标的

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 服务类别 | 服务项 | 服务数量 | 计价单位 | 报价单位 |
| 计算服务  存储服务（兼容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% ） | 2387 | 1CPU | 元/月 |
| 内存 | 5670 | 1GB | 元/月 |
| 普通存储（单盘技术指标:单盘IOPS2000-5000） | 46662 | 1GB | 元/月 |
| 存储服务 | 高性能存储（单盘技术指标：单盘IOPS10000-25000） | 145460 | 1GB | 元/月 |
| 静态存储，提供大容量、高可靠的数据存储服务，具备PB级线性扩展能力 | 70 | 1GB | 元/月 |
| 本地备份服务 | 700 | 1GB | 元/月 |
| 异地备份服务 | 700 | 1GB | 元/月 |
| 网络服务（兼容X86、ARM、C86） | 互联网链路带宽 | 1988 | 1Mb | 元/月 |
| 互联网IP地址租用服务、并提供备案服务 | 42 | 1个 | 元/月 |
| 主机负载均衡服务 | 7 | 1个 | 元/月 |
| 远程接入服务 | 63 | 1个 | 元/月 |
| SSL VPN接入 | 210 | 1个 | 元/月 |
| IPSec VPN接入 | 70 | 1个 | 元/月 |
| 针对网站及Web应用系统提供应用层安全防护，支持各类SQL注入、XSS攻击、网页木马、WEBSHELL等Web威胁防护（200Mbps） | 7 | 1台 | 元/月 |
| 云主机深度监控服务 | 147 | 1台 | 元/月 |

2. 项目背景

北京市疾病预防控制中心（以下简称“市疾控中心”）是根据国务院关于卫生监督、卫生防病体制改革的总体要求，在北京市卫生防疫站、北京市劳动卫生与职业病防治研究所、北京市健康教育所、北京市性病防治所的基础上组建的市级卫生事业单位，承担着北京市传染性疾病、慢性非传染性疾病、学生常见病、病媒生物传播疾病等预防与控制，突发公共卫生事件应急处置和疫情报告和信息管理，食品卫生、环境卫生、放射卫生和职业卫生等健康危害因素的监测与干预，全市居民的健康教育与健康促进和科研教学等工作。

为实现电子政务集约化建设和管理,充分发挥北京市市级政务云(以下简称政务云)的作用,为政务大数据应用奠定基础,依据《国务院关于促进云计算创新发展培育信息产业新业态的意见》(国发〔2015〕5号)和相关政策法规,按照市领导《关于报审电子政务网络升级改造实施方案的请示》的批复精神，“各部门尽可能上云，特例要报批”的要求，结合实际情况，依照国家及北京市统一协调部署，市疾控中心已将北京市人口死亡登记信息系统部署在政务云环境，整体运行良好，根据《国家信息化领导小组关于加强信息安全保障工作的意见》（中办发〔2003〕27号）、《国家政务信息化项目建设管理办法》（国办发〔2019〕57号）、《北京市市级政务云管理办法》的相关管理办法和安全服务保障要求，市疾控中心需要为入云后的信息系统租用云上基础资源和扩展资源等服务，确保市疾控中心死亡登记业务顺利开展，提升信息系统安全保障能力。

**二、商务要求**

1 交付（实施）的时间（期限）和地点（范围）

交付（实施）的时间（期限）：7个月

交付（实施）的地点（范围）：政务云机房

2.付款条件（进度和方式）

详见合同。

**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，对入云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。

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

1. 《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）
2. 《国家政务信息化项目建设管理办法》（国办发〔2019〕57号）
3. 《政府采购需求管理办法》(财库〔2021〕22号)
4. 《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）
5. 《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）
6. 《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）
7. 《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）
8. 《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）
9. 《基于云计算的电子政务公共平台顶层设计指南》
10. 《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）
11. 《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）
12. 《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）
13. 《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）
14. 《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）
15. 《北京市政务网络和数据安全管理办法》（京经信发〔2023〕57号）
16. 《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

1. 《国家电子政务外网安全接入平台技术规范》
2. 《信息技术—云计算—云服务质量评价指标》（GB/T 37738-2019）
3. 《信息技术—云计算—云服务计量指标》（GB/T 37735-2019）
4. 《信息技术—云计算—云服务采购指南》（GB/T 37734-2019）
5. 《信息技术—云计算—云存储系统服务接口功能》（GB/T 37732-2019）
6. 《信息技术—云计算—云资源监控通用要求》（GB/T 37736-2019）
7. 《信息技术—云计算—云平台间应用和数据迁移指南》（GB/T 37740-2019）
8. 《信息技术—云计算—云服务交付要求》（GB/T 37741-2019）
9. 《信息系统灾难恢复规范》（GB/T 20988-2007）
10. 《信息安全技术 云计算服务安全能力要求》（GB/T 31168-2014）
11. 《信息安全技术 网络安全等级保护定级指南》（GB/T 22240-2020）
12. 《信息安全技术 网络安全等级保护基本要求》（GB/T 22239-2019）
13. 《信息安全技术 网络安全等级保护测评要求》（GB/T 28448-2019）
14. 《信息安全技术 信息系统密码应用基本要求》（GB/T39786-2021）
15. 《信息安全技术 信息安全风险评估方法》（GB/T 20984-2022）
16. 《信息安全技术 云计算服务安全指南》（GB/T 31167-2014）
17. 《信息安全技术 政府网站云计算服务安全指南》（GB/T 38249—2019）
18. 《信息安全技术 云计算安全参考架构》（GB/T 35279—2017）
19. 《信息安全技术 云计算服务安全能力评估方法》GB/T 34942—2017
20. 《信息安全技术 云计算服务运行监管框架》（GB/T 37972—2019）
21. 《信息技术 云资源监控指标体系》（GB/T 37938-2019）
22. 《电子信息系统机房设计规范》（GB50174-2017）
23. 《数据中心电信基础设施标准》（ANSI/TIA-942）
24. 《综合布线系统工程设计规范》（GB 50311—2016）
25. 《云计算关键领域安全指南V4.0》

1.2.3北京市相关标准

1. 《政务云平台建设技术要求》（DB11/T 2169-2023）
2. 《北京市政务云安全技术规范 IaaS云计算平台分册》
3. 《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》
4. 《北京市政务云安全技术规范 信息安全服务接口分册》

1.2.4其他

《北京市市级行政事业单位云计算服务框架协议采购项目（2023 年度）》征集文件第四部分采购需求中技术要求

**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/货物技术要求

2.1采购标的需满足的服务标准、期限、效率等要求

2.1.1云主机服务

**（1）服务内容**

按照采购人的具体需求，提供主机服务，包括：x86平台云主机服务，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。

**（2）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. 支持异构虚拟化能力，如KVM多种虚拟化技术；
6. 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；
7. 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；
8. 云计算资源性能要求包括但不限于如下：

* 物理服务器 CPU 主频应不低于2.40GHz；
* 主机内存硬件配置不低于DDR4-2400MHz；
* 可用性不低于99.99%。

2.1.2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、本地备份服务和异地备份服务，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）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：

* 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。
* 支持高可靠性，可靠性不低于99.9999%；

2.1.3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，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. 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。
4. VPN服务，用户通过SSL VPN访问业务系统。

**（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. 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. 应采用集群部署网络控制，以保障升级时业务不中断；
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；
5. 可支持IPv6地址分配，满足业务系统IPv6要求；
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；
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；
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。
9. 网络系统性能要求包括但不限于如下：

* 云内骨干线路带宽不低于10Gb/s；
* 服务器业务带宽不低于1Gb/s；
* 平均可用性不低于99.9%。

1. 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；
2. 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。

2.1.4基础软件支撑服务

**（1）服务内容**

按照采购人的有关管理规定及具体需求，提供商用操作系统、商用应用中间件、商用数据库等软件支撑服务。

**（2）服务标准**

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、Linux操作系统的各种主流版本，并提供操作系统的安装部署和各种故障处理。

1. 商用应用中间件套餐

提供主流商用中间件服务，并提供中间件的安装部署以及各种故障处理和日常维护。

1. 商用数据库套餐

提供商用数据库服务，提供数据库的安装部署和各种故障处理及日常维护。

2.1.5安全服务

**（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，防止重要或敏感数据泄露或被滥用，并建立应急处置体系。安全服务主要内容包含：

1. 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。

1. 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。

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。

1. 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。

1. 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。

1. 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。

1. 主机漏洞扫描

基于漏洞数据库，通过扫描等手段对主机安全脆弱性进行检测。

**（2）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。
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，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/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；
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。

2.1.6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。

**（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3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. 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 。
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。
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。
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。
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。

2.1.7备份服务

**（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。

**（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:

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。
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。

2.1.8日志服务

**（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：

1. 提供收集面向主机的日志服务；
2. 提供对日志的可视化管理、组合过滤查询的能力；
3. 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。

**（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。

2.1.9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。

**（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：

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。

2.1.10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：

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。
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。
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。
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。
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。

2.2采购标的的其他技术、服务等要求

2.2.1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。

2.2.2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。

3.验收标准

3.1服务绩效指标

3.1.1云服务全年整体可用性≥99.9%；

3.1.2故障响应率100%；

3.1.3应急响应时间≤15分钟；

3.2项目验收要求

采购人在服务期满后 15 个工作日内对投标人服务情况进行验收。投标人应当在验收前向采购人提交验收材料。验收合格的，采购人在验收材料上盖章或签字；验收不合格的，投标人应当在【5】日内进行返工或调整，并重新提交采购人验收。

4.服务保障要求

4.1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。

4.2投标人须提供1名项目经理及6名项目团队专职人员，为本项目提供服务。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3年及以上类似工作经验 | 1、项目经理（1名）：具备信息系统项目管理师证书、高级计算机网络工程师证书。  2、系统架构设计师（1名）：具备系统架构设计师证书。  3、数据库管理工程师（1名）：具备高级数据库管理工程师证书及高级信息安全管理工程师。  4、网络工程师（2名）：具备网络工程师证书。  5、售后运维服务人员（2名）：具备软件工程师证书。 |
| 项目  人员 | 6 | 本科及以上 | 有3年及以上类似工作经验 |

4.3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。