**第五章 采购需求**

1. **采购清单：**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **序号** | **采购标的名称** | **数量** | **单位** | **备注** |
| 1 | 政务云基础服务 | 1 | 项 |  |
| 2 | 政务云相关服务 | 1 | 项 |  |

**采购明细:**

**1、政务云基础服务**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 序号 | 服务项 | 服务描述或规格型号 | 服务期 | 价格单位 | 计量单位 | 数量 |
| 一 | 计算服务 |  |  |  |  |  |
| 1-1 | vCPU | 主频不低于2.4GHz | 12月 | 元/月 | 1CPU | 1535 |
| 1-2 | 内存 | 内存 | 12月 | 元/月 | 1GB | 6144 |
| 二 | 存储服务 |  |  |  |  |  |
| 2-1 | 普通性能存储 | 提供普通性能存储服务 | 12月 | 元/月 | 1GB | 74520 |
| 2-2 | 高性能存储（政务外网） | 提供高性能存储服务 | 12月 | 元/月 | 1GB | 4915 |
| 2-3 | 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） | 12月 | 元/月 | 1GB | 19031 |
| 2-4 | 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 | 12月 | 元/月 | 1TB | 251 |
| 三 | 网络服务 |  |  |  |  |  |
| 3-1 | 远程接入服务（政务外网） | 远程接入运维，每个账号结合身份验证，通过VPN远程接入堡垒机进行维护（免费提供1个账号） | 12月 | 元/月 | 1账号 | 1 |
| 3-2 | VPN服务（政务外网） | SSL VPN接入 | 12月 | 元/月 | 1个 | 1 |
| 3-3 | WAF防护（政务外网） | web应用防火墙服务 | 12月 | 元/月 | 1IP | 1 |
| 3-4 | WAF防护 | web应用防火墙服务 | 12月 | 元/月 | 1IP | 1 |
| 四 | 云主机深度监控服务 |  |  |  |  |  |
| 4-1 | 特定云主机深度监控及运维保障服务（7×24小时值守）（政务外网） |  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。 | 12月 | 元/月 | 1主机 | 6 |

**2、政务云相关服务**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 序号 | 服务项 | 服务描述或规格型号 | 服务期(年或月) | 价格单位 | 计量单位 | 数量 |
| 一 | **基础软件支撑服务** |  |  |  |  |  |
| 1-2 | 开源操作系统套餐 | 提供开源操作系统安装和维护服务 | 12月 | 元/月 | 1主机 | 189 |
| 1-3 | 开源数据库套餐 | 开源数据库安装及维护服务 | 12月 | 元/月 | 1套 | 5 |
| 二 | **安全服务** |  |  |  |  |  |
| 2-1 | 主机防护 | 主机防护，每年不少于4次 | 1年 | 元/台・年 | 1台 | 189 |
| 2-2 | 云端APT防护服务 | 对未知攻击威胁进行检测和防护，发现隐蔽威胁、木马后门等异常威胁。 | 12月 | 元/套・月 | 1套 | 2 |
| 2-3 | 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，每年不少于4次 | 1年 | 元/台・年 | 1台 | 189 |
| 2-4 | 主机安全加固 | 针对漏扫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，每年不少于4次 | 1年 | 元/台・年 | 1台 | 189 |
| 2-5 | 网页篡改服务 | 网页篡改服务 | 12月 | 元/月 | 1监控点 | 2 |
| 三 | **安全检测监测、审计服务** |  |  |  |  |  |
| 3-1 | 主机漏洞扫描 | 为用户提供针对主机层面的安全扫描服务，并反馈相关结果，每年不少于4次 | 1年 | 元/台・年 | 1台 | 189 |
| 3-2 | 数据库审计服务 | 支持Oracle、SQL-Server、DB2、MySQL等数据库审计。（1套为1个数据库实例），每年不少于4次 | 1年 | 元/套・年 | 1套 | 5 |
| 3-3 | 主机日志分析 | 主机日志分析，每年不少于4次 | 1年 | 元/台・年 | 1台 | 189 |

**二、项目背景或简况**

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）等文件的要求，开展本单位政务云服务项目。

通过租用北京市级政务云服务，包括租用政务云基础服务资源中的计算服务、存储服务、网络服务、云主机深度监控服务和租用政务云相关服务资源中的基础软件支撑服务、安全服务、安全检测监测审计服务，租用符合最高法院标准的政务云保障法官办案和法院审判职能工作运转，租用政务外网端政务云，服务于向各市级委办局提供数据共享和业务交互。

**三、服务期**

服务期限：12个月。

服务地点：投标人提供的符合北京市级政务云服务的机房

**四、技术参数要求**

1. **政务云租赁服务**
2. 整体要求

投标人提供的云平台整体可用性不低于99.99%，数据可靠性不低于99.9999%。

1. 独立云资源环境

投标人为本项目提供的云资源物理空间独立，并与其他用户的机柜机架、网络设备、网络电路等实现物理隔离，提供不少于25个连续机柜，并预留连续机柜扩展性，配备专门的人防、物防设施并接受采购人的管理。

1. 计算服务

按照采购人的具体需求，提供计算服务，包括：云主机服务租用服务，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需做好与采购人和对应项目应用开发厂商的协调沟通工作，支持完成应用上云工作。

1. 存储服务

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与采购人和对应项目应用开发厂商的协调沟通工作。

1. 网络服务

按照采购人的具体需求，提供网络服务，需具备北京法院专网云网互联接入能力，支持全市现有24条法院专网线路接入，并提供承诺函，支持远程接入服务，VPN服务，WAF防护。在提供服务的过程中需做好与采购人的协调沟通工作。

1. 基础软件支撑服务

按照采购人的有关管理规定及具体需求，提供操作系统套餐和数据库套餐服务。

1、操作系统套餐

按照采购人的有关管理规定及具体需求，提供操作系统套餐服务。

2、数据库套餐

按照采购人的有关管理规定及具体需求，提供数据库套餐服务。

1. 安全服务

云安全应全面符合最高法院相关网络安全管理要求，按照采购人的有关管理规定及具体需求提供安全服务，物理安全方面应提供法院专用政务云物理空间和专用机柜，网络安全服务内容包含不限于主机防护、云端APT防护服务、主机杀毒服务、主机安全加固、网页防篡改服务。

1、主机防护服务

按照采购人的具体需求，提供主机防护服务。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。

2、云端APT防护服务

按照采购人的具体需求，提供云端APT防护服务，对未知攻击威胁进行检测和防护，发现隐蔽威胁、木马后门等异常威胁。

3、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。

4、主机安全加固

按照采购人的具体需求，提供主机安全加固服务，针对预警自查、漏扫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。根据业务系统运行的实际需求，原则上每台服务器服务标准为一年不少于4次。

5、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. 安全检测监测、审计服务

按照采购人的有关管理规定及具体需求提供安全检测、监测、审计服务，服务内容包含主机漏洞扫描、主机日志分析、数据库审计服务。

1、主机漏洞扫描

按照采购人的具体需求，为用户提供针对主机层面的安全扫描服务，并反馈相关结果。根据业务系统运行的实际需求，原则上每台服务器服务标准为一年不少于4次。

2、主机日志分析

按照采购人的具体需求，提供主机日志分析服务。

3、数据库审计服务

按照采购人的具体需求，提供数据库审计服务。

1. 个性化服务

1、业务拓展保障服务

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。

1. 服务期限内，投标人能积极配合采购人对业务应用系统运维开展的提供支撑服务。
2. **服务要求**

（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。

（2）服务方式

投标人提供驻场项目经理1名及项目团队专职人员，提供云平台7×24监控服务。需按照采购人要求，承担云资源服务保障具体工作，项目团队人员需遵守北京市高级人民法院信息化运维人员各项管理要求，在项目实施过程中未经采购人同意，不得随意更换。

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。

投标人负责设立技术支持热线，并安排专人值守，为运维工作提供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。

（3）安全及保密要求

投标人须严格遵守采购人的相关信息安全规定，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。

（4）响应的及时性

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小时内到达运维现场提供服务。系统发生宕机问题时，投标人应在5分钟内响应，在1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。

（5）重点保障要求

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。

1. **安全及扩展要求**

（1）安全要求

投标人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，应能满足安全三级等保要求，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、密码评估、检查、整改等工作。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。

（2）扩展要求

投标人应按照各系统的特点灵活调整计算、存储和带宽等各类资源供给，并能够根据业务数据的变化及时调整存储空间，确保系统高峰时段或特殊时期的访问需求。

1. **业务连续性要求**

投标人需编制业务连续性服务方案包括不限于系统部署、系统测试、系统切割、与采购人现有机房的数据联通性等重点环节。

本项目如涉及系统迁移，在业务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）政务云资源配置、应用迁移、数据迁移、迁移测试、风险评估、迁移期间安全保障、迁移期间应急保障、迁移期间运维保障等内容。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，包含但不限于法院专网及政务外网IP变更割接、业务数据同步及切换上线、功能业务验证及回退等，进行风险评估，提出详细解决方案。

★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，积极与原业务厂商对接，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”并加盖公章。**

**五、售后服务及培训要求**

投标人提供7×24技术支持，为采购人提供良好的咨询服务。保证系统7×24小时不间断稳定运行，系统故障时间原则上不能超过1小时。

投标人应提供云服务操作手册，并为采购人及采购人相关信息化应用运维团队提供必要的使用培训。

**六、验收服务要求**

服务期届满，投标人按照采购人要求完成所有项目服务内容，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。

**七、付款方式**

分期支付。首期付款：于财政资金到位并合同签订后30个工作日内，支付比例不低于合同金额的50%，支付首款。尾款：财政资金到位并提交所有项目成果并验收合格后30个工作日内，支付其余金额。

**八、其他相关要求**

（1）投标人应根据购买服务情况，提交云运维报告、日志审计报告和数据库审计报告，并进行总结分析。

（2）投标人需纳入北京市高级人民法院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。

（3）投标人应每月反馈购买服务的总体使用情况，以及各系统的使用情况。

（4）投标人应配合开展安全审计、资产使用核查、威胁分析、安全检查、事件处置、风险隐患整改等工作。

（5）投标人应配合开展延期服务工作，在本服务期届满时应保障服务的延续性并配合本项目新中标人开展相关工作，保障服务内容不中断、服务质量不下降。

九、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。