**第五章 采购需求**

**一、采购标的**

1. **采购标的（货物需求一览表或简要服务内容及数量）**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **序号** | **货物或服务名称** | **数量** | **单位** | **备注（核心产品）** |
| 1 | 北京市总工会2025年政务云服务云计算服务采购项目 | 1 | 套 | 政务云服务 |

1. **项目背景/项目概述**

依据《关于加快政务信息系统入云工作的函》,目前北京总工会（以下简称“市总工会”）已完成业务系统入云工作。在2025年度，市总工会将继续按照《北京市市级政务云管理办法》中的要求，做好入云业务系统在政务云中的稳定运行保障

市总工会已入云的业务系统包括基层组织建设系统、12351职工服务热线、劳模管理系统、税务代收管理系统、职工服务平台、财务内控一体化系统、大数据平台、法律服务系统、官网、信息报送系统等，提供安全稳定的云资源服务和扩展服务。

目前云资源服务共租用云主机361台、物理服务器2台，包括CPU 3435、内存 8999G、存储 171504G等；扩展服务包括云端APT服务、主机杀毒服务、网页防篡改服务、主机漏洞扫描服务、数据库审计服务、主机安全加固服务、主机日志分析服务、主机防护服务，SDH以太网专线、视频会议服务、强身份认证服务、签名验签服务、加解密服务、时间戳服务、SSL安全服务等。

**二、商务要求**

1. **交付（实施）的时间（期限）和地点（范围）**

服务期为自合同签订之日起12个月。

项目履约地点：采购人指定的地点。

1. **付款条件（进度和方式）**

计划分3次支付。合同生效后按双方约定采购人向中标人支付第一笔项目款，合同执行中期按双方约定采购人向中标人支付第二笔项目款，合同到期且通过验收后采购人向中标人支付剩余项目款。

**三、技术要求**

1. **基本要求**
   1. **采购清单**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **序号** | **服务类别** | **服务子类** | **服务项** | **计价单位** | **报价单位** | **数量** |
| 1 | 计算服务 | x86平台云主机服务 | vCPU（主频不低于2.4GHz） | 1 CPU | 元/月 | 3435 |
| 2 | 内存 | 1 GB | 元/月 | 8999 |
| 3 | 物理服务器 | CPU 2\*E5-2680-V3，内存128GB，硬盘2\*480GB SSD RAID1，万兆网卡2块 | 1台 | 元/台/月 | 2 |
| 4 | 存储服务 | 普通性能存储 | 普通存储（单盘技术指标: 单盘IOPS 2000-5000 ） | 1 GB | 元/月 | 171504 |
| 5 | 本地备份服务 | 本地备份服务 | 1GB | 元/月 | 171504 |
| 6 | 网络服务 | 互联网链路服务 | 互联网链路带宽 | 1 Mb | 元/月 | 550 |
| 7 | 互联网IP地址租用服务、并提供备案服务 | 1 IP | 元/月 | 34 |
| 8 | 主机负载均衡服务 | 主机负载均衡服务 | 1 IP（内网） | 元/月 | 22 |
| 9 | 远程接入服务 | 远程接入服务 | 1账号 | 元/月 | 43 |
| 10 | VPN服务 | SSL VPN接入 | 1套 | 元/月 | 64 |
| 11 | WAF防护 | web应用防火墙服务 | 1 IP（互联网） | 元/月 | 26 |
| 12 | 云主机深度监控服务 | 特定云主机深度监控及保障服务（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 | 361 |
| 13 | 基础软件支撑服务 | 商用操作系统套餐 | 国产操作系统等租用安装服务 | 1个云主机 | 元/月 | 361 |
| 14 | 安全服务 | 云端APT防护服务 | 云端APT防护服务 | 1套 | 元/月 | 4 |
| 15 | 主机杀毒服务 | 主机杀毒服务 | 1台 | 元/月 | 361 |
| 16 | 主机防护 | 主机防护 | 1台 | 元/月 | 157 |
| 17 | 主机安全加固 | 主机安全加固 | 1台 | 元/次 | 39 |
| 18 | 网页防篡改服务 | 网页防篡改服务 | 1监控点 | 元/月 | 28 |
| 19 | 安全检测监测、审计服务 | 主机漏洞扫描 | 主机漏洞扫描 | 1台 | 元/次 | 361 |
| 20 | 主机日志分析 | 主机日志分析 | 1台 | 元/次 | 167 |
| 21 | 数据库审计服务 | 数据库审计服务 | 1套 | 元/月 | 14 |
| 22 | 其它服务 | SDH | 2M SDH 以太专线 | 1条 | 元/年 | 2 |
| 23 | 视频会议 | 云视频会议 | 1点 | 点/月 | 30 |
| 24 | 强身份认证服务 | 数字证书的应用登录认证、服务（10000 次/小时） | 1套 | 元/套 | 1 |
| 25 | 签名验证服务 | 应用中业务数据签名/验证服务（10000 次/小时） | 1套 | 元/套 |
| 26 | 加解密服务 | 为版式文件提供签章服务 | 1套 | 元/套 |
| 27 | 时间戳服务 | 面向业务系统，通过云服务的模式提供时间戳签名服务，务系统通过API接口直接调用本服务实现对业务数据的时间戳签名及验证 | 1套 | 元/套 |
| 28 | SSL安全服务 | SSL安全服务、密码服务（面向业务系统，基于SSL/TLS提供传输加密身份鉴别、SSL卸载、SSL加壳等功能。）。 | 1套 | 元/套 | 1 |
| 29 | 证书服务 | 3个互联网证书，6个政务外网证书。 | 1套 | 元/套 | 9 |
| 30 | 域名服务 | 一级域名服务 | 1套 | 元/套 | 4 |

1. **服务内容及要求**
   1. **云服务能力要求**
      1. **云主机服务要求**

|  |  |
| --- | --- |
| **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，如国产操作系统等，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. **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 |

* + 1. **本地备份服务**

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（不包含备份存储空间费用），默认提供非结构化数据保护、国产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）支持国产操作系统、Linux等主流系统操作系统、国产主流等数据库软件、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。

云服务商应提供对备份过程状态、备份结果提供监控保障云服务，确保备份任务执行成功以及备份的数据完整性。

* + 1. **互联网链路服务**

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

* + 1. **主机负载均衡服务**

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

* + 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 |
| 服务审计 | 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； |
| 可基于账号的登陆时间和资产登陆时间进行访问控制； |
| 可基于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； |

* + 1. **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 |

* + 1. **WAF防护**

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

* + 1. **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 |

* + 1. **商用操作系统套餐**

提供主流商业操作系统服务，应支持国产操作系统和Windows Server、Linux等各种主流版本，并提供操作系统的安装部署和各种故障处理。

* + 1. **云端APT防护服务**

通过APT防护服务，实现恶意代码检测、恶意软件检测及攻击溯源。

* + 1. **主机杀毒服务**

通过杀毒软件，对云主机进行定期的病毒查杀，杀毒软件集中控制。

* + 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. **主机安全加固服务**

根据主机漏洞扫描结果对操作系统暴露的安全问题进行系统加固。

* + 1. **网页防篡改服务**

通过防篡改软件对网站页面进行实时防护，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。

* + 1. **主机日志分析服务**

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。

* + 1. **数据库审计服务**

对数据库操作行为进行细粒度审计的合规性管理，对数据库遭受到的风险行为进行告警，对攻击行为进行阻断。对用户访问数据库行为的记录、分析和汇报，生成合规报告以及事故追根溯源。

* + 1. **SDH专线服务**

提供2M SDH 以太专线专线服务，保障数据传输稳定可靠，支持灵活的带宽配置和快速开通。

* + 1. **视频会议**

提供稳定、高清的云视频会议服务，支持多终端接入，具备会议录制、共享等功能，满足远程协作需求。

* + 1. **强身份认证服务**

提供基于数字证书登录业务应用服务，实现用户端基于数字证书的用户登录，保证用户的身份鉴别的真实性和完整性。

* + 1. **签名验证服务**

提供针对应用中数据的签名验签服务，实现业务系统基于SM2、HMAC-SM3密码算法的数据完整性保护功能。

* + 1. **加解密服务**

需对业务数据提供加解密服务，确保数据存储过程的机密性。

* + 1. **时间戳服务**

提供针对应用中数据的可信时间源服务，以保证在敏感操作的时间真实性和有效性。

* + 1. **SSL安全服务**

提供基于国产算法 SSL服务，密码服务，建立安全 https 通信，保证通信数据的安全性。

* + 1. **证书服务**

提供采用国产密码算法验证网站所有单位的真实身份的标准型 SSL 证书。

* + 1. **域名服务**

提供全面的域名服务。

* 1. **安全管理能力要求**

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。

* 1. **业务连续性服务保障要求**

本项目涉及的业务系统均为采购人在用系统，目前已在北京市市级政务云平台上平稳运行，因此业务连续性是首要的保障需求。

中标后如需将本项目中应用系统迁移至中标服务商云平台中，为保障应用系统迁移过程中的可用性和完整性，对迁移服务的具体要求如下：

（1）迁移进度要求

在合同签订后1个月内，根据采购人需求完成政务云测试、试运行、系统迁移上线工作，并且不能改变和影响采购人原有系统的功能、技术状态、数据完整性。供应商提供承诺函并加盖供应商公章。

（2）迁移经验要求

供应商需具备政府系统政务云迁移经验，可根据业务特点制定应用系统迁移部署方案，明确迁移部署流程、迁移部署保障、迁移部署工具，配合用户完成系统迁移部署、运行和安全保障，迁移过程中保证应用系统不中断。供应商提供迁移承诺函并加盖供应商公章。

（3）迁移费用要求

为确保迁移过程中数据不丢失、系统业务不中断，本次中标人应负责与原政务云平台的服务商进行主动对接，系统迁移所需各项费用（包括但不限于中标人迁移测试阶段的云资源费用及调试费用等），由本次中标人负责解决并包含在本次投标报价中。投标人提供承诺函并加盖投标人公章。

* 1. **保障服务要求**
     1. **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。

* + 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。

* + 1. **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。

* + 1. **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。

* + 1. **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。

* + 1. **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。

* + 1. **人员稳定性要求**

为保障北京市总工会业务云上系统安全稳定高可用运行，需配备专职人员为本项目服务。

* 1. **服务团队要求**

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（高级）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。

* + 1. **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），需具有五年及以上工作经验，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。

* + 1. **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、CISP。

1. **验收标准**

3.1.中标人为采购人提供的服务质量应符合国家或相关行业，以及《北京市市级政务云管理办法》及北京市总工会管理相关要求。

3.2.中标人在按合同要求提供各项服务并形成服务报告文档后，在系统运行正常的前提下，由采购人进行验收。中标人需提供最终签署的合同中约定的相关文档并配合采购人验收工作。