**第五章 采购需求**

1包

**#为重要条款，投标人应根据要求提供证明材料，否则无法得分。**

1. **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 | 云计算服务1包 | 1 | 套 | 政务云基础和扩展服务 |

2. 项目背景/项目概述

依据北京市经信局相关管理规定，北京市总工会业务系统已经部署在北京政务云环境内，为保障已入云业务系统在政务云中的信息系统安全、可靠、稳定运行、继续租用北京市政务云平台，并根据实际需要配置安全服务项目。保障业务系统的在政务云环境内的连续性和可靠性。

1. **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。

2. 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甲方向乙方支付第一笔项目款，合同执行中期按双方约定甲方向乙方支付第二笔项目款，合同到期且通过验收后甲方向乙方支付剩余项目款。

1. **技术要求**

1.项目目标

本项目的服务目标是通过租用市级政务云服务，搭建满足市总工会入云系统安全稳定基础运行环境，并满足相应安全等级保护要求，同时在政务云平台上已完成的基础服务内容的基础上开展进一步的安全防护与优化改造，充分优化系统整体健壮性，提高系统安全性和可靠性，并为应用系统运行提供良好的技术保障。

2.服务内容及要求/货物技术要求

2.1服务内容

为保证市总工会各信息系统入云后的正常运行，未来一年各系统的基础环境将继续依托于我市市级政务云平台，租用政务云基础、扩展服务，具体服务内容及数量如下：

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 序号 | 货物或服务名称 | 数量 | 单位 | 备注（核心产品） |
| 1 | x86平台云主机服务 | 1328 | 1 CPU | （vCPU（主频不低于2.4GHz） |
| 2 | x86平台云主机服务 | 2469 | 1 GB | （内存） |
| 3 | 物理服务器 | 2 | 1台 | CPU 2\*E5-2680-V3，内存128GB，硬盘2\*480GB SSD RAID1，万兆网卡2块 |
| 4 | 普通性能存储 | 30218 | 1 GB | 普通存储（单盘技术指标: 单盘IOPS 1000-3000 ） |
| 5 | 高性能存储 | 8704 | 1 GB | 高性能存储（单盘技术指标：单盘IOPS 3000-20000 ） |
| 6 | 集中存储 | 1630 | 1 GB | 提供用于共享磁盘的集中存储服务，用于oracle rac环境 |
| 7 | 静态存储 | 28438 | 1 TB | 大容量、高可靠的数据存储服务，具备PB级线性扩展能力，提供静态数据存储 |
| 8 | 互联网链路带宽 | 500 | 1 Mb | 互联网链路带宽 |
| 9 | 互联网IP地址租用服务、并提供备案服务 | 25 | 1 IP | 互联网IP地址租用服务、并提供备案服务 |
| 10 | 主机负载均衡服务 | 20 | 1 IP（内网） | 主机负载均衡服务 |
| 11 | 远程接入服务 | 26 | 1账号 | 每个账号结合身份验证通过VPN远程接入堡垒机进行维护 |
| 12 | VPN服务 | 26 | 1套 | 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。 |
| 13 | WAF防护 | 25 | 1 IP（互联网） | 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。 |
| 14 | 特定云主机深度监控及运维保障服务（7\*24小时值守） | 100 | 1主机 | 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 |
| 15 | 商用操作系统套餐 | 99 | 1云主机 | Windows Server套餐：Windows Serve、国产操作系统租用、安装及维护。 |
| 16 | 云端APT防护服务 | 3 | 1套 | 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。 |
| 17 | 主机杀毒服务 | 274 | 1台 | 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。 |
| 18 | 网页防篡改服务 | 25 | 1监控点 | 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。 |
| 19 | 主机漏洞扫描 | 274 | 1台 | 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。 |
| 20 | 数据库审计服务 | 13 | 1套 | 支持Oracle、SQL-Server、DB2、MySQL、国产数据库等数据库审计。 |
| 21 | 本地备份服务 | 30000 | 1GB | 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） |
| 22 | 主机安全加固 | 35 | 1台 | 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。 |
| 23 | 主机日志分析 | 50 | 1台 | 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 |
| 24 | 主机防护 | 40 | 1台 | 主机防护：提供符合等保三级要求的主机权限管理及安全防护。 |
| 25 | SDH | 2 | 1条 | 2M SDH 以太专线 |
| 26 | 视频会议 | 30 | 点/月 | 云视频会议 |
| 27 | 强身份认证服务 | 2 | 项/年 | 面向业务系统，通过云服务的模式提供基于数字证书的强身份认证服务，本服务支持单独验证签名、验证签名+验证证书、单独验证证书三种应用模式，本服务可以配合移动个人签名服务、USBKey证书、服务器证书完成移动端、PC端以及业务服务之间的强身份认证。 |
| 28 | 签名验证服务 | 2 | 项/年 | 面向业务系统，通过云服务的模式提供签名验签服务，该服务可以为业务系统免费提供单位证书，由本单位的业务系统通过API接口直接调用本服务实现对业务数据的签名验签。 |
| 29 | 加解密服务 | 2 | 项/年 | 面向业务系统，通过云服务的模式提供加解密服务（包括对称加解密、数字信封加解密），该服务可以为业务系统免费提供单位证书，由本单位的业务系统通过API接口直接调用本服务实现对业务数据的加解密。 |
| 30 | 时间戳服务 | 2 | 项/年 | 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。 |
| 31 | SSL安全服务（国密） | 2 | 项/年 | 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。 |
| 32 | 国密SSL证书 | 2 | 张/年 | 支持360、奇安信等国密浏览器的SM2算法OV SSL证书。OV SSL证书是指验证网站所有单位的真实身份的标准型SSL证书，通过证书颁发机构审查网站企业身份和单域名或多域名的所有权以证明申请单位是一个合法存在的真实实体。 |
| 33 | 云服务接入集成费 | 1 | 项 | 提供应用系统接入云服务所需应用集成、开通和配置服务 |

2.1.1、计算服务

按照采购人的有关管理规定及应用系统对计算资源的具体需求，实现对各应用系统合理的计算资源配置。

2.1.2、存储服务

按照采购人的有关管理规定及应用系统对存储资源的具体需求，实现对各应用系统合理的存储资源配置。

2.1.3、网络服务

按照采购人的有关管理规定及应用系统对网络资源的具体需求，实现对各应用系统合理的网络资源配置。

2.1.4、云主机深度监控服务

按照采购人的有关管理规定及应用系统对主机监控的具体需求，实现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。

2.1.5、安全服务

按照采购人的有关管理规定及具体需求，提供云端APT防护服务、主机杀毒服务、网页防篡改服务等安全防护服务，实现对各应用系统合理的服务配置。

供应商应保证业务应用系统的支撑环境，包括但不限于服务器、网络、存储等相关物理环境能满足安全等保要求，依据招标需求向采购人提供本次项目中所涉及安全服务内容。

同时供应商需提供完整、可行的安全防护设计方案，为用户系统下一步进行信息系统安全等级保护测评提供支撑。

2.1.6、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，提供主机防护、主机漏洞扫描、主机安全加固、数据库审计服务、主机日志分析、本地备份服务等安全检测服务，实现对各应用系统合理的服务配置。

2.1.7、其他服务

依据GB/T 39786《信息安全技术 信息系统密码应用基本要求》标准进行密码应用安全性建设。为满足上述系统的安全需求，需采购包括强身份认证服务、签名验证服务、加解密服务、时间戳服务、SSL安全服务（国密）、国密SSL证书等在内的密码云服务，增强信息系统安全性，将密码安全服务覆盖信息系统的全流程环节，实现业务过程中的身份鉴别、抗抵赖、防篡改、数据完整性校验，有效防止内容否认和行为否认，实现任何操作和行为均可追溯，保证信息系统数据的真实性、有效性、保密性、合法性，为北京市总工会信息化系统业务发展提供安全保障。

2.2服务要求

**#2.2.1、迁移要求**

中标后需将本包件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）迁移经验要求

供应商需具备国家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，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。**

（2）迁移进度要求

在合同签订后10日内，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。**

（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。**供应商提供承诺函并加盖供应商公章。**

2.2.2、安全及扩展要求

（1）安全要求

按照采购人的有关管理规定及各个应用系统的需求，供应商需提供对各应用系统安全保障服务，并在此基础上提供其它安全保障服务，以满足系统上云后的全方位安全防护需求。

（2）扩展要求

供应商应按照各系统的特点灵活调整计算资源、存储资源及网络资源等各类服务供给，并能够根据业务保障的需要灵活调整基础资源，确保系统高峰时段或特殊时期的访问需求。

2.2.3、运维服务要求

（1)服务规范

供应商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

供应商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。

供应商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。供应商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

供应商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

供应商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，供应商应在5分钟内响应，供应商须具备故障快速定位和恢复能力，故障定位排除时限不超过30分钟，重要信息系统故障定位排除时限不超过10分钟，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。

（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，要求供应商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。

2.2.4、考核要求

根据采购人的考核要求，按照制定的绩效考核指标体系及服务承诺要求，接受采购人对其服务质量的考核。

2.2.5、其他要求

供应商需提供1名项目负责人（项目经理）及10名以上具有项目经验的项目团队专职人员，为本项目提供实施服务工作。项目经理需具有10年以上工作经验并同时具备高级信息系统项目管理师证书。项目团队人员（除项目经理之外）具备CISP证书。

供应商需承诺若需要进行系统迁移，系统迁移在合同签订后10日内完成，每延误一天扣除合同总额的1%作为违约金。在完成系统迁移之前，供应商应支付原服务商云服务费用，费用金额按照(中标价/365)\*原服务商提供云服务的天数进行支付。

供应商需承诺云平台服务可用性高于99.99%，数据持久性高于99.9999%。违约则按照违约条款赔偿。

**2.3 需要由供应商提供的设计方案、解决方案或组织方案**

2.3.1总体服务方案：包括云平台数据保护功能；计算服务、存储服务、网络服务和云主机深度监控服务等基础服务方案；主机杀毒、漏洞扫描、安全加固、软件租用等扩展等。

2.3.2部署方案：根据实际情况制定部署方案，评估部署过程中可能遇到的风险，明确迁移部署所需时间。如须迁移，还需提供采购人要求的承诺函。

2.3.3安全服务方案：包括对于采购人业务系统安全防护、安全技术保障措施等。

2.3.4运维服务方案：包括服务规范、服务方式、安全及保密、响应的及时性、重点保障等。

2.3.5服务保障：通过制度、辅助措施等手段，确保各项服务能够保质保量完成。

3. 验收标准

供应商所提供资源应满足磋商文件规定的要求。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12小时。服务期满后30个工作日开始对合同项目进行验收。成交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. 其他要求

本项目所需政务云平台需通过网络安全等级保护三级测评，能够提供相关证明并加盖报价人公章。

采购需求

2包

**#为重要条款，投标人应根据要求提供证明材料，否则无法得分。**

1. **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 | 云计算服务2包 | 1 | 套 | 政务云基础和扩展服务 |

2. 项目背景/项目概述

依据北京市经信局相关管理规定，北京市总工会业务系统已经部署在北京政务云环境内，为保障已入云业务系统在政务云中的信息系统安全、可靠、稳定运行、继续租用北京市政务云平台，并根据实际需要配置安全服务项目。保障业务系统的在政务云环境内的连续性和可靠性。

1. **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。

2. 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甲方向乙方支付第一笔项目款，合同执行中期按双方约定甲方向乙方支付第二笔项目款，合同到期且通过验收后甲方向乙方支付剩余项目款。

1. **技术要求**

1.项目目标

本项目的服务目标是通过租用市级政务云服务，搭建满足市总工会入云系统安全稳定基础运行环境，并满足相应安全等级保护要求，同时在政务云平台上已完成的基础服务内容的基础上开展进一步的安全防护与优化改造，充分优化系统整体健壮性，提高系统安全性和可靠性，并为应用系统运行提供良好的技术保障。

2.服务内容及要求/货物技术要求

2.1服务内容

为保证市总工会各信息系统入云后的正常运行，未来一年各系统的基础环境将继续依托于我市市级政务云平台，租用政务云基础、扩展服务，具体服务内容及数量如下：

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **序号** | 货物或服务名称 | 数量 | 单位 | 备注（核心产品） |
| 1 | x86平台云主机服务 | 969 | 1CPU | vCPU（主频不低于2.4GHz） |
| 2 | x86平台云主机服务 | 2167 | 1GB | 内存 |
| 3 | 普通性能存储 | 15284 | 1GB | 普通存储（单盘技术指标: 单盘IOPS 1000-3000 ） |
| 4 | 高性能存储 | 61508 | 1GB | 高性能存储（单盘技术指标：单盘IOPS 3000-20000 ） |
| 5 | 静态存储 | 14 | 1TB | 大容量、高可靠的数据存储服务，具备PB级线性扩展能力，提供静态数据存储 |
| 6 | 互联网链路服务 | 50 | 1Mb | 互联网链路带宽 |
| 7 | 9 | 1IP | 互联网IP地址租用服务、并提供备案服务 |
| 8 | 主机负载均衡服务 | 2 | 1IP（内网） | 主机负载均衡服务 |
| 9 | 远程接入服务 | 17 | 1账号 | 每个账号结合身份验证通过VPN远程接入堡垒机进行维护 |
| 10 | VPN服务 | 38 | 1套 | 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。 |
| 11 | WAF防护 | 1 | 1IP（互联网） | 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。 |
| 12 | 特定云主机深度监控及运维保障服务（7\*24小时值守） | 91 | 1主机 | 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 |
| 13 | 商用操作系统套餐 | 22 | 1个云主机 | Windows Server套餐：Windows Server、国产操作系统租用、安装及维护。 |
| 14 | 云端APT防护服务 | 1 | 1套 | 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。 |
| 15 | 主机杀毒服务 | 117 | 1台 | 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。 |
| 16 | 网页防篡改服务 | 3 | 1监控点 | 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。 |
| 17 | 主机漏洞扫描 | 4 | 1台 | 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。 |
| 18 | 数据库审计服务 | 1 | 1套 | 支持Oracle、SQL-Server、DB2、MySQL、国产数据库等数据库审计。 |
| 19 | 本地备份服务 | 15277 | 1GB | 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） |
| 20 | 主机安全加固 | 4 | 1台 | 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。 |
| 21 | 主机日志分析 | 117 | 1台 | 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 |
| 22 | 主机防护 | 117 | 1台 | 主机防护：提供符合等保三级要求的主机权限管理及安全防护。 |
| 23 | 强身份认证服务 | 2 | 项 | 面向业务系统，通过云服务的模式提供基于数字证书的强身份认证服务，本服务支持单独验证签名、验证签名+验证证书、单独验证证书三种应用模式，本服务可以配合移动个人签名服务、USBKey证书、服务器证书完成移动端、PC端以及业务服务之间的强身份认证。 |
| 24 | 签名验证服务 | 2 | 项 | 面向业务系统，通过云服务的模式提供签名验签服务，该服务可以为业务系统免费提供单位证书，由本单位的业务系统通过API接口直接调用本服务实现对业务数据的签名验签。 |
| 25 | 加解密服务 | 2 | 项 | 面向业务系统，通过云服务的模式提供加解密服务（包括对称加解密、数字信封加解密），该服务可以为业务系统免费提供单位证书，由本单位的业务系统通过API接口直接调用本服务实现对业务数据的加解密。 |
| 26 | 时间戳服务 | 2 | 项 | 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。 |
| 27 | SSL安全服务（国密） | 2 | 项 | 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。 |
| 28 | 国密SSL证书 | 2 | 张 | 支持360、奇安信等国密浏览器的SM2算法通过证书颁发机构审查网站企业身份和单域名或多域名的所有权以证明申请单位是一个合法存在的真实实体。 |
| 29 | 云服务接入集成费 | 1 | 项 | 提供应用系统接入云服务所需应用集成、开通和配置服务 |

2.1.1、计算服务

按照采购人的有关管理规定及应用系统对计算资源的具体需求，实现对各应用系统合理的计算资源配置。

2.1.2、存储服务

按照采购人的有关管理规定及应用系统对存储资源的具体需求，实现对各应用系统合理的存储资源配置。

2.1.3、网络服务

按照采购人的有关管理规定及应用系统对网络资源的具体需求，实现对各应用系统合理的网络资源配置。

2.1.4、云主机深度监控服务

按照采购人的有关管理规定及应用系统对主机监控的具体需求，实现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。

2.1.5、安全服务

按照采购人的有关管理规定及具体需求，提供云端APT防护服务、主机杀毒服务、网页防篡改服务等安全防护服务，实现对各应用系统合理的服务配置。

供应商应保证业务应用系统的支撑环境，包括但不限于服务器、网络、存储等相关物理环境能满足安全等保要求，依据招标需求向采购人提供本次项目中所涉及安全服务内容。

同时供应商需提供完整、可行的安全防护设计方案，为用户系统下一步进行信息系统安全等级保护测评提供支撑。

2.1.6、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，提供主机防护、主机漏洞扫描、主机安全加固、数据库审计服务、主机日志分析、本地备份服务等安全检测服务，实现对各应用系统合理的服务配置。

2.1.7、其他服务

依据GB/T 39786《信息安全技术 信息系统密码应用基本要求》标准进行密码应用安全性建设，为满足系统的安全需求，需采购包括强身份认证服务、签名验证服务、加解密服务、时间戳服务、SSL安全服务（国密）、国密SSL证书等在内的密码云服务，增强信息系统安全性，将密码安全服务覆盖信息系统的全流程环节，实现业务过程中的身份鉴别、抗抵赖、防篡改、数据完整性校验，有效防止内容否认和行为否认，实现任何操作和行为均可追溯，保证信息系统数据的真实性、有效性、保密性、合法性。

2.2服务要求

**#2.2.1、迁移要求**

中标后需将本包件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）迁移经验要求

供应商需具备国家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，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。**

（2）迁移进度要求

在合同签订后10日内，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。**

（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。**供应商提供承诺函并加盖供应商公章。**

2.2.2、安全及扩展要求

（1）安全要求

按照采购人的有关管理规定及各个应用系统的需求，供应商需提供对各应用系统安全保障服务，并在此基础上提供其它安全保障服务，以满足系统上云后的全方位安全防护需求。

（2）扩展要求

供应商应按照各系统的特点灵活调整计算资源、存储资源及网络资源等各类服务供给，并能够根据业务保障的需要灵活调整基础资源，确保系统高峰时段或特殊时期的访问需求。

2.2.3、运维服务要求

（1)服务规范

供应商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

供应商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。

供应商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。供应商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

供应商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

供应商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，供应商应在5分钟内响应，供应商须具备故障快速定位和恢复能力，故障定位排除时限不超过30分钟，重要信息系统故障定位排除时限不超过10分钟，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。

（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，要求供应商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。

2.2.4、考核要求

根据采购人的考核要求，按照制定的绩效考核指标体系及服务承诺要求，接受采购人对其服务质量的考核。

2.2.5、其他要求

供应商需提供1名项目负责人（项目经理）及10名以上具有项目经验的项目团队专职人员，为本项目提供实施服务工作。项目经理需具有10年以上工作经验并同时具备高级信息系统项目管理师证书。项目团队人员（除项目经理之外）具备CISP证书。

供应商需承诺若需要进行系统迁移，系统迁移在合同签订后10日内完成，每延误一天扣除合同总额的1%作为违约金。在完成系统迁移之前，供应商应支付原服务商云服务费用，费用金额按照(中标价/365)\*原服务商提供云服务的天数进行支付。

供应商需承诺云平台服务可用性高于99.99%，数据持久性高于99.9999%。违约则按照违约条款赔偿。

**2.3 需要由供应商提供的设计方案、解决方案或组织方案**

2.3.1总体服务方案：包括云平台数据保护功能；计算服务、存储服务、网络服务和云主机深度监控服务等基础服务方案；主机杀毒、漏洞扫描、安全加固、软件租用等扩展等。

2.3.2部署方案：根据实际情况制定部署方案，评估部署过程中可能遇到的风险，明确迁移部署所需时间。如须迁移，还需提供采购人要求的承诺函。

2.3.3安全服务方案：包括对于采购人业务系统安全防护、安全技术保障措施等。

2.3.4运维服务方案：包括服务规范、服务方式、安全及保密、响应的及时性、重点保障等。

2.3.5服务保障：通过制度、辅助措施等手段，确保各项服务能够保质保量完成。

3. 验收标准

供应商所提供资源应满足磋商文件规定的要求。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12小时。服务期满后30个工作日开始对合同项目进行验收。成交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. 其他要求

本项目所需政务云平台需通过网络安全等级保护三级测评，能够提供相关证明并加盖报价人公章。