##  采购需求

### 项目背景

 本次项目建设宜兴市政务云计算平台同城异地备份中心，是为了深入贯彻落实《网络安全法》和国家网络等级保护制度，切实强化宜兴市政务云计算平台的网络安全工作，保障云上政务应用、公共数据的安全管理。当前，宜兴市云计算中心已入驻44家单位（部门及乡镇、园区、街道）115个应用系统。总体来看，政务云平台实施了政务网络安全云平台、政务云数据安全等项目建设，基本实现了政务云平台及其数据资源的安全管理，并为云平台各租户单位提供多类型、个性化的安全产品服务。但云中心安全体系还需要进一步强化，特别是政务云平台同城异地备份。云上部署了大数据平台、公共健康云平台、教育云平台等重要信息化系统，汇聚了人口、法人、信用等城市基础数据库和专题数据库大量的数据资源。当意外或故障发生时，异地备份可以保障政务云平台的核心系统和数据资源能通过备份系统迅速恢复对外应用服务，实现业务连续性，确保数据资源完好无损，保证宜兴政务云平台健壮、可靠的运行。

宜兴政务云同城异地备份中心平台的搭建将有助于与宜兴电子政务从粗放式、离散化的建设模式向集约化、整体化的可持续发展模式转变，使政府管理服务从各自为政、相互封闭的运作方式向跨部门跨区域的协同互动和资源共享转变。

第二节 采购需求方案

请在下方提供经工信局审核通过的项目建设方案，若采购单位擅自变更项目采购内容及投资额，财政部门将终止采购活动。

### 项目内容

宜兴政务云同城异地备份中心采用政府按需采购服务，企业投资、建设、运营云计算中心模式，利用虚拟化、分布式等云计算技术，为政府各部门提供数据、系统等业务的备份容灾及计算、存储、网络等弹性、可靠、安全的信息化基础设施服务。

通过公开招投标确定宜兴政务云同城异地备份中心的供应商与云备份服务单价。

### 总体要求

完成宜兴市电子政务应用的同城异地备份中心的系统设计、软硬件集成及系统实施、运行维护等工作，为宜兴市提供专业、安全、高效的云计算服务，优化完善宜兴市电子政务云计算服务平台。

要求云计算服务能力可弹性扩展，可满足未来三年宜兴市电子政务和智慧城市建设发展的需要。确保在此期间，宜兴市电子政务应用和智慧城市应用能够按照要求稳定运行。

政务云计算同城异地备份中心需具备对现有政务云平台中的各类业务系统和数据进行备份的能力。

中标单位须免费为云服务使用单位提供系统迁移服务。

整体项目建设原则如下：

（1）可恢复性

备份的目的就是为了恢复，如果备份成功率不可预知或不能保证在合理的时间范围内恢复系统数据，备份系统就没有价值。如果备份系统发生硬件或软件故障，有流程但没有经过演练甚至没有相应的故障恢复流程，系统很可能得不到迅速的恢复，降低应用系统的可用性。

（2）系统整体的均衡

应该对备份系统各部分都进行性能估算，使备份系统不产生明显的瓶颈。所有备份恢复负载应均衡到不同的网卡、交换机、磁带驱动器等。追求局部性能而忽视整体的均衡实际上达不到高性能。

（3）安全性

对于备份网络的组网设计，安全性是非常重要的，如防止发生网络风暴、黑客入侵和病毒入侵等，在设计备份网络的时候要充分考虑到各种安全隐患，通过实施网络隔离、分层防护等手段，保证业务系统的网络安全。

（4）易管理性

备份系统是IT系统中极为重要的一部分，应尽量采取集中统一的管理方式，实现性能监控、配置动态变更等功能。

（5）可扩展性，动态扩展能力

备份系统可以方便地扩充、升级，可以满足现在乃至未来较长一段时间内的增长需求，保护用户现有的投资，结构上能方便的过渡到LAN-Free/ServerFree的备份方案。

### 初始规模

本项目中标人在合同签订生效后三个月内，为本项目建设的电子政务云计算平台资源池的规模须不低于：800vCPU（主频不小于2.0GHz，复用率≤1.5），3000GB内存（内存不允许复用方式分配资源，性能不低于DDR4 2133MHz）,50TB存储，后期根据电子政务应用的实际需求进行扩容。

### 报价要求

本次投标报价须为折扣报价，投标人针对本项目云服务目录及限价报出整体折扣（折扣是指，如投标人报价为95折，即在《开标一览表》中填列95%，则投标人各单项报价=目录单项限价×95%），不得针对单项服务报价。根据折扣报价计算的云计算服务价格包含服务费、税费等其它所有费用。

中标人的投标报价为本项目合同执行期间提供云服务的最高限价。

### 云服务目录

根据宜兴市电子政务发展的实际需求，宜兴市电子政务同城异地备份中心云服务目录及投标限价如下表所示：

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **序号** | **服务类别** | **服务项** | **详细需求** | **单位** | **限价（元）** |
| 1 | 云备份容灾服务 | 业务数据备份服务 | 分布式并行存储（1TB） | 月 | 253 |
| 磁盘阵列存储(1TB) | 月 | 782 |
| 监控存储（配企业级硬盘）(1TB) | 月 | 118 |
| 虚拟机整机备份服务 | 4核（≥2.0GHz），8GB内存，160GB硬盘（SAS/SATA≥7200rpm） | 月 | 621 |
| 4核（≥2.0GHz），16GB内存，160GB 硬盘（SAS/SATA≥7200rpm） | 月 | 996 |
| 8核（≥2.0GHz），16GB内存，160GB 硬盘（SAS/SATA≥7200rpm） | 月 | 1150 |
| 8核（≥2.0GHz），24GB内存，160GB 硬盘（SAS/SATA≥7200rpm） | 月 | 1801 |
| X86整机备份服务 | 2颗CPU(每CPU≥六核不低于2.0GHz)，32GB内存，3\*300G硬盘（SAS/SATA≥7200rpm） | 月 | 1502 |
| 4颗CPU(每CPU≥六核不低于2.0GHz)，64GB内存，3\*300G硬盘（SAS/SATA≥7200rpm） | 月 | 3373 |
| 20核（2.2GHZ）128GB内存，3\*600GB 10K SAS盘，2\*10GE光口（含光模块）+2\*GE | 月 | 3066 |

### 技术要求

宜兴政务云计算同城异地备份中心为宜兴市电子政务提供的云服务内容包括但不限于以下资源服务：

云备份容灾服务

提供X86/虚拟机整机、业务系统、数据备份服务（文件、数据库、操作系统），需支持Oracle、SQL Server等常用的数据库系统、支持windows2008、centos7等主流操作系统。

提供备份文件验证功能、可开启一个虚拟化验证主机，提供备份数据去重与合并功能、提供WindowsSever、windows和linux备份代理程序，提供无系统X86/虚拟机/云主机裸机、WindowsSever、linux、windows还原代理、可实现单/批量文件恢复和下载、提供异构主机间的全量和快速灾难恢复功能，备份数据可挂载恢复到云主机。

（1） 计算资源服务

包括虚拟主机和物理服务器，满足电子政务多样化需求。

（2） 存储资源服务

包括通用光纤存储、闪存高速存储、分布式存储、云盘存储等存储服务。

（3） 网络资源服务

提供对服务器进行流量分发的负载均衡服务。

（4） 基础安全服务

提供基础安全服务，主要包括主机防病毒服务。

（5） 增强租户安全服务

提供增强租户安全服务，包括云防火墙服务、主机安全服务、云数据库审计服务、云web应用防火墙服务、云堡垒机服务、日志审计服务和数据保护服务。

（6） 云平台安全服务

提供云平台安全服务，主要提供漏洞扫描服务、网页防篡改服务和安全问题应急响应服务。

（7） 安全服务组合版

基础安全服务组合A包括：主机安全（5节点）、云防火墙（1000M）、日志审计（5节点、100GB存储空间）、云堡垒机（5节点）和云web应用防火墙。

基础安全服务组合B包括：主机安全（3节点）、云防火墙（1000M）。

（8） 运维服务

包括运维标准规范、运维管理系统、运维技术团队、运维保障、资源变更、业务系统测试支持、定时巡检、应急管理、现场值守等服务。

（9） 机房资源服务

投标人或其总公司须拥有自建机房。机房位于宜兴市行政区域范围内，且已具备双线路不同管网和路由的政务外网接入能力。机房基础环境符合国家机房相关标准，提供完善的空调、供配电、防雷接地、消防等基础环境设施服务，提供42U标准机柜，满足设备托管要求。机房至少需接入双路市电，机柜配置双PDU并分别接入一路市电，机房配备UPS、柴油发电机等应急设施。

（11） 增强安全资源池

投标人须构建符合国家和省相关要求的增强安全资源池，提供符合国家和省相关要求的主机服务。增强安全资源池须使用符合国家和省相关要求的产品和技术，不受限于其他参数要求。

#### 总体架构要求

宜兴政务云同城异地备份中心需要基于业内领先的多云架构，具备相应的云管能力，通过云管系统实现对本云计算资源的统一管理，同时具备可无缝接入统一纳管平台的能力。

要求中标单位提供的云计算平台、虚拟化平台、网络、安全、存储系统等在保证各自独立性的前提下实现深度融合，保证整体技术架构的灵活性、先进性、合理性、高可用、高安全和可扩展性。

云平台需通过至少两条冗余的裸光纤接入宜兴市电子政务外网网络核心，云计算服务需包含云主机备份服务，备份策略至少应满足每天一次增量备份，备份还原点不少于15个。

政务云计算同城异地备份中心提供的云计算服务，需为用户提供操作系统等安装介质，配合完成系统安装，操作系统、数据库等软件序列号由最终云服务使用单位提供。

宜兴政务云同城异地备份中心需在云平台网络边界部署IPS、WAF、防火墙等安全设备提供边界防护，云平台须满足信息系统安全等级保护2.0标准三级的要求。

宜兴政务云同城异地备份中心需要分为安全出口区、核心交换区、计算资源区、存储区、运维管理区。

安全出口区需求：分别需要提供互联网、电子政务外网出口南北向流量安全管控，根据不同网络出口的要求设置不同的安全设备与安全策略，提高业务网络的安全性以及业务连续性。

核心交换区需求：核心交换区需要负责汇聚整个数据中心高性能数据转发。核心交换区是一个高速的二层交换骨干。设计时通过设备冗余、路由冗余、链路冗余等技术，充分保障网络系统稳定性。

核心交换机配置两台核心交换机做虚拟化，提供高可靠的数据转发服务，并旁挂负载均衡，完成整个数据中心流量的链路负载。

链路容灾需求，同城异地备份中心与政务外网需要双芯裸光纤高速网络连接，同城数据中心之间采用IP网络连接，网络带宽要保证系统切换的顺畅和数据复制的带宽需求。

计算资源区：实际业务承载区，根据业务的不同划分为等保2级区和等保3级区，各区部署X86服务器并通过虚拟化集群提高业务可用性。计算资源区设置数据备份区，数据备份区可进行数据备份防止病毒、人为逻辑错误，保障用户数据高可靠。

存储需求区：存储区为用户业务数据需求提供存储服务，依据用户业务的不同需求设置集中式存储、备份存储。并通过FC SAN网络和IP网络上联计算资源区。

运维管理区需求：运维管理区需要提供整个云政务的管理运维、保障服务，设置SDN控制器、云计算管理平台、综合运维平台、虚拟化管理平台、日志审计、堡垒机、漏洞扫描。

政务云计算同城异地备份中心的网络必须通过冗余裸光纤接入宜兴市电子政务外网网络核心，经由宜兴市电子政务外网实现与各委、办、局，互联网，各专网连通并为宜兴市各委、办、局提供云计算服务。政务云计算同城异地备份中心各数据中心内部网络应能满足电子政务发展需要，所有网络设备均需实现冗余，并配备相应的电信级安全设备保证数据中心的安全。

#### 基础设施服务（IaaS）要求

##### 云备份容灾服务要求

政务云计算同城异地备份中心需为宜兴市电子政务提供云备份容灾服务，提供的云备份容灾服务主要包括：基础备份服务和业务数据备份服务。各业务部门的重要数据需各业务部门自行备份。政务云计算同城异地备份中心提供的备份服务需满足的要求如下：

(一) 业务数据备份服务要求

（1）提供业务数据备份服务：为防止数据库误操作、关键文件误删除等操作导致业务系统崩溃，需提供业务数据备份服务；

（2）支持虚拟机备份服务：对虚拟机的镜像进行备份，支持用户自定义备份频率及数量，恢复时间视虚拟机镜像的大小而定；

（3）支持操作系统备份：对服务器的操作系统进行完整备份，支持用户自定义备份频率及副本数量，恢复时间视操作系统的大小而定；

（4）支持文件备份：对常见文件系统中的某个文件进行备份，支持用户自定义备份频率及副本数量，恢复时间视文件的大小而定；

（5）支持Oracle、SQL Server、MySQL等常见数据库备份，支持用户自定义备份频率及副本数。

（二）业务系统灾备服务要求

（1）整机全场景灾备保护：

具备对业务系统进行整机全场景的保护的能力。保护内容为整个生产环境，包括OS、应用系统、配置文件、中间件等所有数据，保证数据一致性和完整性；

（2）业务灾难快速应急接管：

提供故障业务快速拉起接管功能，当连续性要求较高的业务中断但无可用的恢复平台时，灾备云可将故障业务在1-2分钟内拉起并正常提供服务。

（3）分钟级快速重建，保障业务连续性：

业务系统突发任何软件故障、硬件故障、逻辑错误、病毒攻击等导致业务系统中断，可以在做15分钟的快速重建，保障业务的连续性；

在进行业务系统重建时，无需人工手工的重建操作系统、业务软件、数据库，建立数据库连接关系等复杂耗时的操作过程，通过简单的几个步骤完成业务系统的快速恢复，有效应对业务系统突发故障时的业务中断问题。

（4）微秒级CDP持续数据保护，保障数据完整性：

对业务系统增量数据做持续的CDP数据保护，可保证任意时间点的数据不会丢，保证了数据的完整性。

（5）异构环境兼容性保护和跨平台重建恢复：

实现任意品牌技术的虚拟化平台和物理主机平台上的业务系统的数据保护；

实现在任意品牌技术的虚拟化平台和物理主机异构平台之间的快速重建和迁移。打通虚拟化环境与物理主机平台间的业务屏蔽性。

（6）分钟级灾难演练：

分钟级别的将重要的业务系统进行快速重建到虚拟化平台或者时物理主机上，进行灾难演练，无需调整拓扑，设计演练方案、演练模拟等耗时耗力等复杂过程。快速、方便的检验系统的可靠性，满足等保2.0的新要求。

（7）任意时间点文件验证：

可对保护的业务系统数据实现任意时间点的验证，直接可以找到任意时间点的数据，直观看到保护的数据状态，可以查找到不同时间点不同状态的数据，并可以将数据拷贝出来直接使用。应对对文件出现的误删、误改、误操作等一系列逻辑错误都可以及时有效的应对。

（8）任意时间点系统验证：

可对保护的业务系统通过自启动虚拟化平台的方式进行系统验证，管理员可像真实生产环境一样登陆查看数据和各应用可用性，确保系统的可靠性；

##### 计算资源服务要求

政务云计算同城异地备份中心需通过构建计算资源池的方式为宜兴市电子政务提供计算资源服务，提供的计算资源服务主要包括：虚拟主机、物理服务器以及按需配置的CPU、内存、GPU卡、硬盘、网络接口等。计算资源服务需要满足的要求如下（增强安全资源池使用符合国家和省相关要求的产品和技术，不受限于其他参数要求）：

(一) 虚拟主机要求

（1）提供可动态、弹性扩展的虚拟主机资源；

（2）应可按照需求创建虚拟主机，安装操作系统；

（3）虚拟机能根据用户需求提供接入电子政务外网服务；

（4）虚拟机模板设计应考虑计算能力、存储空间、快速部署和定制化要求；

（5）虚拟主机CPU主频不小于2.0GHz；

（6）内存不允许复用方式分配资源，性能不低于DDR4 2133MHz；

（7）系统盘不低于60G，数据盘按需可选；

（8）支持虚拟机的日常管理操作，能够完全释放虚拟机资源；

（9）支持某一宿主机发生故障时，虚拟机系统自动迁移至新宿主机；

（10）支持虚拟机快照管理及回滚，支持虚拟机迁移，实现故障自动恢复。

(二) 物理服务器要求

（1）按需提供企业级物理服务器资源；

（2）按需为物理服务器配备x86架构CPU，单个CPU主频不低于2.0GHz；

（3）按需为物理服务器增配内存，内存规格不低于DDR4 2666MHz；

（4）按需为物理服务器配备企业级物理硬盘，提供三种规格的物理硬盘：

① 物理硬盘A：3.5吋7.2K SAS/SATA盘；

② 物理硬盘B：2.5吋10K SAS盘；

③ 物理硬盘C：2.5吋SSD盘。

（5）按需为物理主机配备网络接口，包括千兆网络接口和万兆网络接口。

(三) 计算资源池技术要求

（1）虚拟化软件架构须采用裸金属架构，必须能直接安装在服务器硬件设备上，不能采用在服务器上先安装操作系统的方式，虚拟化软件要能直接管理硬件资源；

（2）支持虚拟机远程挂载光驱功能：支持虚拟机在运行情况下，管理员将本地PC、本地服务器或者本地虚拟机的光驱设备或者镜像文件（ISO9660格式）挂载到虚拟机中，进行虚拟机操作系统或者软件的安装、修复；

（3）支持虚拟机CPU/内存热添加，当虚拟机操作系统不支持CPU/内存热添加时，支持重启虚拟机操作系统而不是停止启动虚拟机，使得热添加的CPU/内存生效；

（4）删除用户磁盘时，支持选择是否彻底清除磁盘数据，避免利用工具对数据进行恢复，以保证数据的安全；

（5）支持虚拟机HA功能：虚拟化系统在服务器硬件故障导致虚拟机宕机的情况下，可自动地将虚拟机在其它正常的服务器启动，尽快恢复虚拟机上业务运行；

（6）支持存储迁移功能：支持虚拟机关机或开机情况下，虚拟机的卷迁移至其他存储单元中，可以在存储虚拟化管理下的同一个存储设备内、不同存储设备之间进行迁移。

##### 存储资源服务要求

政务云计算同城异地备份中心需通过构建存储资源池的方式为宜兴市电子政务提供存储资源服务，提供的存储资源服务主要包括：磁盘阵列存储、闪存高速存储、分布式存储、云盘存储等。存储资源服务需要满足的要求如下：

(一) 磁盘阵列存储要求

（1）基于模块化设计、高可靠保障的磁盘阵列，以及全冗余光纤网络构建的存储系统；

（2）使用企业级高速硬盘提供高可靠、高性能的块存储空间；

（3）采用全模块架构冗余设计，无单一故障点；

（4）多控制器架构，最大支持16个控制器，控制器之间支持缓存镜像；

（5）双控制器配置≥64GBCache（非SSD或者高速Flash充当缓存）；

（6）支持SSD二级缓存技术，加上速数据读取速度，降低应用延迟；

（7）IOPS 读 （512b块全顺序读）≥600000；

（8）IOPS 写 （512b块全顺序写）≥400000；

（9）双控最大支持34个主机接口。

(二) 闪存高速存储要求

（1）基于模块化设计、高可靠保障的磁盘阵列，以及全冗余光纤网络构建的存储系统；

（2）使用企业级高速固态硬盘（SSD）提供高可靠、高性能的全闪存块存储空间；

（3）支持多控制器集群架构；

（4）存储系统应为统一存储架构；

（5）支持NAS、FC-SAN、IP-SAN（iSCSI）和FCoE数据访问功能；

（6）NAS功能应为非网关实现方式；

（7）IOPS 读 （512b块全顺序读）≥600000；

（8）IOPS 写 （512b块全顺序写）≥400000；

（9）硬件部件采用全冗余无单点故障设计。

(三) 分布式存储要求

（1）基于分布式架构，支持RESTful API接口，为用户提供海量、安全、高可靠的云存储服务；

（2）分布式架构，性能、容量随节点数增加而线性增加；

(四) 存储资源池技术要求

（1）要求能够保证存储的持久性、数据可销毁性、数据可迁移性、数据私密性；

（2）存储资源可以横向扩展添加新的节点，存储容量可线性地增长。

（3）存储系统采用全冗余架构，当存储系统出现硬件故障时能够确保数据的完整性、可用性。

（4）支持Windows和Linux客户端访问存储；

（5）支持结构化和非结构化数据存储；

（6）支持集中式存储和分布式存储，全面满足各类存储服务对于存储空间、扩展性、读写性能、可靠性等多方面需要；

（7）支持主流的开源数据库、Oracle、SQL Server、MySQL等关系型数据库存储功能；

（8）支持文件、视频等存储功能，支持常见的数据保护功能，保证数据的完整性、一致性；

（9）支持将存储池中的存储空间按用户需求划分为独立的虚拟磁盘或裸盘；

##### 网络资源服务要求

针对宜兴政务云同城异地备份中心平台的安全合规建设需求及安全威胁防范需求，此次需要通过安全云管平台，打造具备完善安全能力的“云网安一体化”云平台。将安全能力与云平台、SDN网络、虚拟化平台等深度融合，并在云平台上呈现唯一用户接口，灵活、高效，实现云安全的整体交付。需要遵循等级保护技术建设“一个中心三重防护”的设计理念，以安全防护、安全检测、安全管理等多个视角，为云平台提供多方位、多角度的安全保护措施构建宜兴平台的安全技术需求体系。



遵循“分区分域”的设计原则，划分安全管理中心、出口安全防护、安全检测、网络资源、租户安全防护、租户安全管理、计算及存储资源、数据安全防护等区域，以政务业务及子系统功能或能力，构建细粒度业务域。

在安全出口防护区部署数据防泄漏、防火墙、入侵防御等设备构建出口安全防护资源池，主要针对互联网及电子政务外网边界进行安全防护与检测，保障边界安全。

在网络资源池区部署安全网关、应用交付系统等构建南北向安全资源池，主要针对各子区域的通信网络安全、区域边界安全进行防护，通过高性能、高吞吐的硬件安全防护设备以及池化的软件资源实现，以实现南北向安全可弹性扩展和按需分配。

在计算及存储资源池区部署安全防护资源池构建东西向安全资源池，主要针对各子区域内部从虚拟化资源、虚拟化服务角度对云计算虚拟化进行安全防护和策略设计，通过虚拟化平台自身的安全机制及VM层安全防护组件（虚拟机隔离、Hypervisor层访问控制、VM系统安全加固等）实现。

构建数据安全防护资源池，主要包括邮件数据防泄漏、应用数据防泄漏、数据备份等设备，实现针对全网核心数据、核心资产的防泄漏管理以及出现数据泄露风险后的回溯与重建，保障全网数据安全。

构建安全管理中心与安全检测资源池，主要承载各类安全管理及安全审计，实现系统管理、审计管理、安全管理能力的集中。同时在安全管理中心、安全检测资源池边界部署防火墙，实现对安管管理及检测区业务的双向访问控制，并以带外管理网络建立起安全的信息传输路径。

政务云计算同城异地备份中心提供流量分发的负载均衡服务，可以通过流量分发扩展应用系统对外的服务能力，通过消除单点故障提升应用系统的可用性。

##### 安全服务要求

政务云计算同城异地备份中心必须纳入宜兴市大数据局统一云管理，并为宜兴市电子政务提供安全服务。政务云计算同城异地备份中心须在云平台网络边界部署IPS、WAF、防火墙等安全设备提供边界防护。政务云计算同城异地备份中心提供的安全服务只是安全防护手段，系统安全责任不因使用云服务而转移，仍由云服务使用单位负责。

根据2019年7月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、财政部颁布的《云计算服务安全评估办法》，为进一步提升党政机关使用云计算服务的安全可控水平，投标人为本项目提供的云计算服务须接受网信办条线部门管理，并通过中央网信办党政部门云计算服务网络安全管理审查（安全能力级别：增强，机房位置在江苏无锡）。

中标供应商在为宜兴市政府单位提供各类云服务之前，政务云计算同城异地备份中心须通过信息安全等级保护（第叁级）评测并取得测评报告。

提供的安全服务主要包括：基础租户安全服务、增强租户安全服务、云平台安全服务和安全服务组合版。提供的安全服务需满足的要求如下：

(一) 基础安全服务

提供基础安全服务，主要包括主机防病毒服务。

(二) 增强租户安全服务要求

提供增强租户安全服务，包括云防火墙服务、主机安全服务、云数据库审计服务、云web应用防火墙服务、云堡垒机服务、日志审计服务和数据保护服务。

(三) 云平台安全服务要求

可提供云平台安全服务，主要提供漏洞扫描服务、网页防篡改服务和安全问题应急响应服务。

(四) 安全服务组合版要求

基础安全服务组合A包括：主机安全（5节点）、云防火墙（1000M）、日志审计（5节点、100GB存储空间）、云堡垒机（5节点）和云web应用防火墙。

基础安全服务组合B包括：主机安全（3节点）、云防火墙（1000M）。

##### 运维服务要求

政务云计算同城异地备份中心需提供完善的技术服务及运维保障服务，包括标准规范、运维管理、运维技术团队、运维保障、资源变更、业务系统测试、定时巡检、应急管理、值守服务等服务。运维服务要求如下：

(一) 标准规范

针对政务云中心的维护管理、运维操作、应急管理以及云服务的申请、交付、保障、监督等流程制定相关规范和标准，并根据实际运行需求进行持续更新和优化。

(二) 运维管理

供应商根据政务云服务的特点，建立完备运维管理体系，标准规范的运维管理制度，明确项目组织管理措施和手段。具备对日常运维管理事务的支撑，包括事件管理、问题管理、变更管理、资产管理等服务管理机制，并根据管理需求的变化进行必要的更新，确保项目实施和运维服务的有效性和服务团队的稳定性。

(三) 运维技术团队

供应商应提供专业的运行维护和技术支持本地团队，配置云计算、网络、存储、安全等方面的专业运维工程师和架构设计师，对人员的录用、离岗、考核、培训进行统一管理，对各专业岗位进行定员定岗，具备高效维护和持续优化的技术能力。

(四) 运维保障

针对机房基础设施、基础IT设备、运维支撑平台等进行日常维护、故障处理以及性能优化，协助用户处理业务系统运行过程中遇到的各种故障与问题。

(五) 资源变更

根据用户需求对CPU核数、内存空间、硬盘等计算资源进行变更。

(六) 业务系统测试

支持用户进行业务系统的功能及性能测试，根据用户需求部署相应的测试环境。

(七) 定时巡检

供应商应制定规范的服务巡检制度，定期针对机房基础设施、基础IT设备、运维支撑平台、关键业务系统进行定时巡检，及时发现系统故障及安全隐患。

(八) 应急管理

制定完善的应急管理制度以及针对各种突发情况的应急预案。

(九) 值守服务

提供7×24小时现场值守服务，及时发现并解决故障或隐患，保证政务云平台的故障及紧急情况能快速发现和解决，随时接收并响应用户的报障及服务要求。

##### 机房资源服务要求

宜兴政务云计算同城异地备份中心机房位于宜兴市行政区域范围内，为保障已上云备份的各类应用系统有一个相对稳定、连续的运行环境，避免由于云计算基础环境的改变，从而导致应用中断、服务停止的风险，机房由投标人（或其总公司）自建而非租赁，已具备政务外网接入条件。

机房基础环境要求符合国家标准GB50174-2008《电子信息系统机房设计规范》中规定。

(一) 基本要求

（1）机房面积不小于400平米（不包含办公用房）；

（2）操作监控区应与其他区之间隔音，操作监控区安装适合人体的普通空调，其他区有机房专用恒温、恒湿空调负责调节，机房信号电缆和电源电缆分层布放，布局美观；

（3）操作监控区安装网管监控设备、开发用机或其他业务操作用机，在操作监控区使用切换器的集中控制功能对工作站和服务器等进行集中管理；

（4）机房云资源服务准备时间不大于5个工作日。

(二) 机柜

机房具备不低于100个42U、4kw的标准机柜，具备按需扩展能力。

(三) 机房装修

（1）机房室内顶棚上安装的灯具、风口、火灾探测器应满足国家相关标准要求；

（2）机房围护结构和材料应满足保温、隔热、防火等要求，墙面应洁白干净。地面和四壁装饰，采用水泥砂浆抹灰。地面材料应平整、耐磨。

(四) 机房供配电

（1）机房所用的交流电源由机房大楼配电房独立回路进行供电，避免受大楼大功率用电设备的影响，保证机房用电设备的稳定运行；

（2）机房需单独设置市电配电箱、UPS/DPS输出配电柜，动力（空调、风机、照明等）用电需与设备用电分开；

（3）机房提供正常照明和应急照明；

（4）提供市电保障，每路容量不小于600KVA，配电系统稳定可靠；

 (五)备用电源系统

 提供冗余电源，备用电源支撑不低于0.5小时；

(六) 机房空调

（1）机房温湿度满足国家机房标准；

（2）机房内设置漏水告警装置；

（3）使用机房恒温、恒湿专用精密空调，配备N+1冗余，保证机房恒温、恒湿，无局部过热。

 (七) 机房消防

（1）机房应符合现行有关国家消防标准的规定；

（2）机房需设专业气体自动灭火系统，并应按现行有关规范的要求执行；

（3）消防器材放置位置醒目；

（4）机房应设火灾自动报警系统，并应符合现行国家标准的规定；

（5）报警系统和自动灭火系统应与空调、通风系统联动；

（6）机房内空调设备应受机房内电源切断开关的控制，机房内的电源切断开关应靠近工作人员的操作位置或主要出入口；

（7）消防系统符合国家现行标准并通过国家消防管理部门验收。

(八) 机房防雷接地

（1）防雷设施满足国家相关规范要求，总配电柜、UPS/DPS配电柜、重要设备输入回路前端安装电源避雷器；

（2）数据信号传输设备采用信号避雷器；

（3）整个机房内作地线排网，设备就近接入；机房内金属墙板、金属顶板、地板支架、金属线槽以及各种电子设备的金属外壳、机架等均需实现接地，保证机房内电力设备、IT设备等免受静电或雷击破坏。

(九) 防静电

（1）机房采用防静电设施，采用活动地板的，活动地板应由阻燃性材料制成，并能够抗静电；

（2）采用保护接地的措施防止静电的发生。

(十) 安全

（1）需设置门禁系统等安全措施，防止任何无关人员进入；

（2）需有防鼠、防虫措施。所有机房进出口桥架、管道出口都要采取密封措施；

(十一) 数据链路

政务云计算同城异地备份中心数据中心铺设两根裸光纤分别连接至市政务外网机房与原数据中心机房的核心交换机。

#### 平台层服务（PaaS）要求

政务云计算同城异地备份中心应具备提供平台层服务（PaaS）的能力，如docker、K8S等。

### 8.项目组人员要求：

结合本项目建设需求，投标人须提供项目建设运维人员配置详单，其中：①项目组负责人1人；②组长1人；③管理、运维人员6人或以上。投标文件中提供投标人（或其下属分支机构）为项目组人员缴纳的投标截止时间前近十二个月中连续三个月社保证明并加盖投标人公章。

第二部分 评标方法和标准

**一、评分项目（总分100分）**

|  |  |
| --- | --- |
| 技术商务部分 | 90分 |
| 价格部分 | 竞争性磋商 | 分 | 价格分值占总分值的比重为10%至30% |
| 公开招标 | 10分 | 价格分值占总分值的比重不得低于10% |

**二、“技术商务部分”评审内容：**

以下两种格式采购人根据主客观因素分布情况自行选择。主客观因素能够进行明显区分的，选用格式1；主客观评审因素杂糅在一起，无法区分开的，选择格式2。

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 评审内容 | 序号 | 评审项目 | 分值 | 评审细则 |
| 主观评审因素 | 1 | 云平台技术方案 | 10 | 要求虚拟化平台、网络、安全、存储系统等在保证各自独立性的前提下实现深度融合，保证整体技术架构的灵活性、先进性、合理性、高可用、高安全和可扩展性。在方案中体现全面且架构合理、功能完善、可扩展性强的得10分；在方案中体现基本合理、功能较完善的得7分；在方案中体现不够全面的得4分；其余情况不得分。 |
| 2 | 服务考核与质量保证 | 10 | 云服务商应提供基于自身云平台的内部规范、规定或预案，其内容应包含但不限于故障处置、应急响应、人员值班管理等。在方案中体现全面且规范合理、突发应对得当的得10分；在方案中体现规范合理且基本全面的得7分；在方案中体现不够全面的得4分，其余情况不得分。 |
| 3 | 运维服务方案 | 10 | 云服务商运维服务方案：云服务商应提供7×24小时响应服务、承诺运维需求平均响应时间小于等于30分钟。在方案中体现全面且运维保障可靠的得10分；方案体现基本全面且运维保障较好的得7分；在方案中体现不够全面的得4分，其余情况不得分。 |
| 客观评审因素 | 1 | 机房参数 | 12 | 1、投标人提供的机房面积大于2000平方米，4KW机架大于200个的得4分（投标文件中需提供证明材料复印件并加盖投标人公章，未提供不得分）2、投标人提供的机房市电保障采用双路市电，两路2000KVA以上市电的得4分（投标文件中需提供证明材料复印件并加盖投标人公章，未提供不得分）3、投标人提供的机房备用电源系统，冗余后备电源大于0.75小时，能提供两台柴油发电机组，功率达到2000KVA以上的得4分（投标文件中需提供证明材料复印件并加盖投标人公章，未提供不得分） |
| 2 | 公司综合实力 | 16 | 1、投标人具有ISO/IEC 20000标准管理体系认证证书的得1.5分，未提供不得分；投标人具有ISO9001:2015标准质量管理体系认证证书的得1.5分，未提供不得分。（投标文件中需提供证明材料复印件并加盖投标人公章，未提供不得分） |
| 2、投标人具有省级及以上企业信用管理贯标证书的得3分，未提供不得分（投标文件中需提供证明材料复印件并加盖投标人公章，未提供不得分）。 |
| 3、投标人有云服务用户数据保护能力服务证书、云缓存服务证书、应用托管容器服务证书、云分发服务证书、云备份服务能力证书，有 1 个得 2 分，最高得 10分（投标文件中需提供工信部相关直属机构出具的证书复印件并加盖投标人公章，未提供不得分） |
| 3 | 项目负责人 | 8 | 投标人为本项目配备项目负责人1名，该名项目负责人具有通信工程高级工程师职称、注册信息安全工程师、信息通信网络机务员证书、全国网络技术水平三级及以上认证证书的，有一个得2分，最多得8分。（投标文件中提供投标人（或其下属分支机构）为其缴纳的投标截止时间前近十二个月中连续三个月份社保证明及相关证书复印件并加盖投标人公章，未提供不得分） |
| 4 | 人员配备-除项目负责人以外的项目组成员 | 24 | 1、投标人为本项目组配备组长1名，该名组长具有中华人民共和国信息产业部颁发的高级程序员证书、注册信息安全专业人员（CISP）证书的，有一个得2分，最多得4分。2、投标人为本项目组配备的团队成员中具有省级及以上公安厅出具的网络信息安全管理员上岗合格证的，有一个得2分，最多得8分。3、投标人为本项目组配备的团队成员自2017年1月1日以来每拿过一个国家级网络安全大赛奖项得2分，最多得6分。4、投标人为本项目组配备的团队成员中具有公安部出具的国家重要信息系统保护人员证书的，有一个得2分，最多得6分。（投标文件中提供投标人（或其下属分支机构）为其缴纳的投标截止时间前近十二个月中连续三个月份社保证明及相关证书复印件并加盖投标人公章，未提供不得分） |