“东莞市政务云平台建设—云服务商资格采购”项目概况其他内容

7 服务要求

7.1 服务范围

本项目服务范围：

1. 按采购人的需求提供计算、存储、网络、备份等服务。
2. 按采购人的需求提供数据库、中间件等服务。
3. 建设满足安全等级保护三级要求的安全运行环境并提供安全服务。
4. 按采购人的需求提供云平台运维服务、技术培训服务以及其他技术服务。

7.2 服务内容

7.2.1 类型一服务

7.2.1.1 基础设施即服务（IaaS）

7.2.1.1.1 计算服务

7.2.1.1.1.1x86 架构虚拟主机服务

要求能够迅速地获得虚拟机设施，并且这些基础设施是弹性的，可以根据需求进行扩展和收缩。包括如下规格及服务：

序号	类型	规格
1	基础型	2 核、4G 内存、100G 硬盘
2		4 核、8G 内存、100G 硬盘
3	通用型	8 核、16G 内存、100G 硬盘
4		16 核、32G 内存、100G 硬盘
5	内存型	2 核、8G 内存、100G 硬盘
6		4 核、16G 内存、100G 硬盘
7		8 核、32G 内存、100G 硬盘
8		16 核、64G 内存、100G 硬盘
9	计算型	32 核、64G 内存、100G 硬盘
10		32 核、128G 内存、100G 硬盘
11	定制化虚拟机（2 核/单位）	提供定制化虚拟机，单台虚拟机的 vCPU 数量最大支持 64 核
12	定制化虚拟机（4G/单位）	提供定制化虚拟机，内存数量最大支持 512G

7.2.1.1.1.2 裸金属服务

裸金属服务要求兼容 ARM、MIPS 架构和 x86 架构,具体要求如下：

序号	类型	规格
1	裸金属服务（ARM、MIPS 架构）	基础型 1（2 路 32 核，CPU 主频≥2.6GHz，内存≥32G）
2		基础型 2（2 路 64 核，CPU 主频≥2.6GHz，内存≥32G）
3	裸金属服务（x86 架构）	基础型 1（4 路 16 核，CPU 主频≥2.3GHz，内存≥32G）
4		基础型 2（2 路 8 核，CPU 主频≥2.1GHz，内存≥32G）

针对裸金属服务器，可选以下配件：

序号	类型	规格
1	裸金属服务可选配件	32G 内存
2		1TB SAS 硬盘
3		1TB SATA
4		1TB SSD 硬盘
5		1T NVME 硬盘
6		HBA 卡

7		万兆网卡（含模块）

7.2.1.1.1.3GPU 资源服务

基于 GPU 的应用主要涵盖视频编解码、深度学习、科学计算等多种场景。要求具有实时高速的并行计算和浮点计算能力、出色的图形处理能力和高性能计算能力提供极致计算性能，有效解放计算压力，提升产品的计算处理效率与竞争力。要求提供多种配置类型的 GPU 显卡供用户选择。

7.2.1.1.1.4 镜像服务

要求提供镜像服务，包括操作系统和预装的软件。通过镜像，实现在虚拟化主机实例上实现应用场景的快速部署。

7.2.1.1.2 存储服务

本次存储资源服务主要提供以下内容：

序号	服务名称	服务规格
1	存储资源服务	普通 IO 云硬盘（100G/单位）
2		高 IO 云硬盘（100G/单位）
3		超高 IO 云硬盘（100G/单位）
4		文件存储服务（100G/单位）
5		对象存储服务（100G/单位）

7.2.1.1.2.1 块存储服务

要求支持用户在申请云主机时可以指定容量大小、存储 SLA（指定存储介质：SATA、SAS、SSD 或 Any，存储 SLA 选项由管理员在资源池下定义）。

本次云硬盘存储服务主要提供以下内容：

序号	服务名称	服务内容
1	普通 IO 云硬盘（100G/单位）	块存储（NL-SAS 盘）,适用于大容量、读写速率中等、事务性处理较少的应用场景。单盘最大 IOPS 为 800。
2	高 IO 云硬盘（100G/单位）	块存储（SAS 盘），适用于主流的高性能、高可靠应用场景。单盘最大 IOPS 为 2500。
3	超高 IO 云硬盘（100G/单位）	块存储（SSD 盘），适用于超高 IO，超大吞吐量的读写密集型应用场景。本期单盘最大 IOPS 为 10000。

7.2.1.1.2.2 文件存储服务

要求提供 NFS（Network File System，网络文件系统）和 CIFS(Common Internet File System，公共互联网文件系统)等异构平台共享文件系统，支持不同类型计算机、操作系统、网络架构和传输协议运行环境中的网络文件远程访问和共享。

具体技术要求如下：

1、文件存储服务要求具备高可用性和持久性，为海量数据、高带宽型应用提供有力支持，适用于多种应用场景，包括媒体处理、文件共享、内容管理和 Web 服务等。

2、单一文件系统存储容量可扩展至≥100PB。

3、支持 NFS（V3/V4），SMB（V1/V2/V3），HDFS（支持与 Cloudera 对接），FTP，NDMP，Amazon S3/OpeanStack Swift 接口；

4、支持单客户端对多个节点进行并发访问，单客户端最大带宽可达 2.5GBps。

5、支持并配置客户端连接负载均衡软件,负载策略支持 CPU 占用率。

6、支持自动精简配置，可按需动态分配存储空间，保证存储资源的最大化利用。

7、支持 N+M 冗余模式。

7.2.1.1.2.3 对象存储服务

要求能够提供海量、安全、高可靠、低成本的数据存储能力，包括：创建、修改、删除桶，上传、下载、复制、修改、删除对象等。

具体技术要求如下：

1、支持创建、删除、查看桶和 AK/SK 密钥。支持桶 ACL 设置、对象 ACL 设置和桶策略设置；

2、支持存储资源池在线扩展；

3、支持数据检查：存储前一致性检查，确保存入数据是上传数据；

4、支持全局命名空间，无需指定 region 即可访问全部桶和对象；

5、生命周期管理：用户可以为某个桶定义生命周期管理规则，来为该桶的对象定义各种生命周期规则；

6、支持查看用户配额（容量）、桶配额（容量）；

7、支持 5TB 的超大文件存储；

8、多版本控制：开启多版本控制后

（1）上传对象时，能够自动为每个对象创建唯一的版本号。上传同名的对象将以不同的版本号同时保存在对象存储中；

（2）可以指定版本号下载对象，不指定版本号默认下载最新的对象。

9、支持大文件分段上传和合并。

10、可批量删除对象。

7.2.1.1.3 网络服务

7.2.1.1.3.1 虚拟私有云

虚拟私有云（Virtual Private Cloud）的技术要求如下：

能够提供安全、隔离的网络环境，为应用或虚拟机提供网络资源，实现应用向云上的平滑迁移。

每个 VDC 至少有一个 VPC，且允许申请多个 VPC，VPC 之间网络空间隔离，部门或组织按业务安全隔离要求规划 VPC。

可以在 VPC 中定义与传统网络无差别的虚拟网络，同时提供 SNAT、多出口访问等高级网络服务，以满足更多的业务部署要求。

用户可以完全掌控自己的虚拟网络，包括创建自己的网络，配置 DHCP（仅 TYPE2 场景）、DNS。

7.2.1.1.3.2 安全组服务

要求安全组实现组内和组间的访问控制，加强虚拟机的安全保护，实现 VPC 内部的网络隔离。

支持将 VPC 内的虚拟机加入一个安全组，然后设定不同安全组间的访问规则。同一个安全组内的地址之间的访问不受限制，默认组间禁止访问。

支持为虚拟机提供粒度的安全访问控制。控制虚拟机网络消息的流入流出，只允许授权的消息通过。当云主机申请成功后，可以将云主机加入到某个安全组内，安全组上配置安全规则。

7.2.1.1.3.3 虚拟防火墙服务

对子网进行访问控制，支持黑白名单（即允许和拒绝策略），根据与子网关联的入方向/出方向 ACL（Access Control List）规则，判断数据包是否被允许流入/流出子网。

要求能够提供多层次、灵活的网络 ACL 功能，通过虚拟防火墙方便地管理 VPC 及子网的访问规则，加强云服务器的安全保护。

7.2.1.1.3.4 弹性 IP

要求实现弹性 IP 服务，要求支持租户将申请的公网 IP（或者政务外网 IP）绑定到虚拟机或者负载均衡器上，从公网（或者政务外网）访问云数据中心内虚拟机。用户对已经申请的弹性 IP，可以执行以下操作：

绑定弹性 IP 地址：将申请到的弹性 IP 地址和路由网络中关联的虚拟机进行绑定，使虚拟机可以通过固定的 IP 地址进行访问。弹性 IP 所在的 VPC 和虚拟机接入网络所在的 VPC 相同。

解绑定弹性 IP 地址：如果虚拟机不再提供服务，或者在服务地址不变的情况下更换业务虚拟机时，用户可以解绑定弹性 IP 地址。

删除弹性 IP 地址：删除不再使用的弹性 IP 地址。如果待删除的弹性 IP 地址已绑定虚拟机，可先解绑定，再删除。

7.2.1.1.3.5 负载均衡

要求能够根据用户设定的负载均衡策略，将业务请求均匀分发到与之关联的云主机上，使得各个云主机的业务负载均衡，保证业务的稳定性和可靠性。

具体技术要求如下：

支持在已创建的 ELB 上管理监听器，包括名称，描述，负载均衡协议及端口，负载均衡算法，会话保持等，并同时创建健康检查。

支持健康检查配置，检查后端云主机的运行状态，包括健康检查协议，检查周期，超时时间，最大轮询次数等，与监听器创建合一。

7.2.1.1.4 硬件托管服务

托管服务主要应用于以下场景：

（1）因各种技术或其他原因，使用单位的应用系统暂时无法迁移到云平台中，但又需要将服务器托管到云平台中。

（2）使用单位所购置服务器使用年限不长，足够支撑现有应用系统的资源需求，但需要将服务器托管到云平台中。

（3）其它特殊专用设备。

各使用单位可以直接租用机柜，将设备托管到中标供应商的机房，完成托管设备上架和网络接入配置，网络设备、安全设备复用云平台使用的设备，可视需要购买安全增值服务。具备如下规格：

序号	服务类型	物理机柜规格
1	云数据中心 1U 机柜	一个标准机柜功率为 6500W,机柜高度为 47U，配备柜顶交换机
2	云数据中心 2U 机柜	一个标准机柜功率为 6500W,机柜高度为 47U，配备柜顶交换机
3	云数据中心 1 个机柜	一个标准机柜功率为 6500W,机柜高度为 47U，配备柜顶交换机

7.2.1.1.5 备份服务

7.2.1.1.5.1 本地（同城）备份服务

在本地（同城）机房提供云平台主机承载的应用文件、数据库，以及云主机的数据备份资源，预防系统故障或数据丢失风险，恢复数据点 RPO<24 小时，恢复时间 RTO<6 小时。

本次政务云按照 1T 备份存储/单位提供本地备份服务。

备份频率：优先按照用户要求进行备份。用户无要求的情况下，每 24 小时至少一次增量（或差异）备份、每周至少一次全量备份。

保存周期：优先按照用户要求进行保存。用户无要求的情况下，备份大于 3 个月。

备份恢复以用户为单位做隔离，每个用户只能访问自己备份数据。

7.2.1.1.5.2 异地备份服务

基于本地备份服务在异地灾备机房提供可恢复的业务数据副本，预防灾难事件下的系统故障或数据丢失风险，恢复数据点 RPO<24 小时，恢复时间 RTO<12 小时。

本次政务云按照 1T 备份存储/单位提供异地备份服务。

备份频率：优先按照用户要求进行备份。用户无要求的情况下,每 24 小时至少一次增量（或全量）备份，每月至少一次全量备份。

保存周期：优先按照用户要求进行保存。用户无要求的情况下，备份大于 6 个月。

备份恢复以用户为单位做隔离，每个用户只能访问自己备份数据。

7.2.1.2 平台即服务（PaaS）

7.2.1.2.1 数据库服务

7.2.1.2.1.1 分布式 MySQL 服务

提供分布式 MySQL 数据库服务，要求可用性≥99.95%，要求兼容 mariadb 10.1、MySQL5.5/5.6/5.7、兼容 x86 架构、ARM 架构。

具体提供的 MySQL 分布式数据库服务规格如下：

序号	规格
1	定制化服务（2 核/单位）
2	定制化服务（4G 内存/单位）
3	定制化服务（100G 存储/单位）

7.2.1.2.1.2 国产关系型数据库服务

要求提供国产关系型数据库服务，提供开即用、稳定可靠、可弹性伸缩的数据库服务。要求具有多重安全防护措施和完善的性能监控体系，并提供专业的数据库备份、恢复及优化方案。

具体提供的国产关系型数据库服务规格如下：

序号	规格
1	定制化服务（2 核/单位）
2	定制化服务（4G 内存/单位）
3	定制化服务（100G 存储/单位）

7.2.1.2.1.3 国产非关系型数据库服务

要求提供国产非关系型数据库服务，提供开即用、稳定可靠、可弹性伸缩的数据库服务。要求具有多重安全防护措施和完善的性能监控体系，并提供专业的数据库备份、恢复及优化方案。

具体提供的国产非关系型数据库服务规格如下：

序号	规格
1	定制化服务（2 核/单位）
2	定制化服务（4G 内存/单位）
3	定制化服务（100G 存储/单位）

7.2.1.2.1.4PostgreSQL 服务

PostgreSQL 分布式关系数据库是基于开源数据库开发的分布式关系数据库集群，作为云资源平台重要的数据库产品能力。要求支持分配 OLTP 类实例或 OLAP 类实例，支持同一份数据支撑 OLTP 类和 OLAP 类负载。其中，OLTP 支持 TPCC 标准测试模型下 TMP Total 300 万以上；支持百 TB 级数据规模和亿级用户访问。

具体提供以下规格的 PostgreSQL 分布式关系数据库：

序号	规格
1	定制化服务（2 核/单位）
2	定制化服务（4G 内存/单位）
3	定制化服务（100G 存储/单位）

7.2.1.2.2 中间件服务

7.2.1.2.2.1 消息中间件

要求提供消息中间件，支持存储进程间传输的消息，为分布式部署的不同应用之间或者一个应用的不同组件之间提供基于消息的可靠的异步通信服务。

7.2.1.2.2.2 分布式服务框架

分布式服务框架是一个围绕应用和微服务的平台，要求提供服务全生命周期管理能力，提供多维度应用、服务、机器的监控数据，助力服务性能优化。要求支持分布式服务发布与注册、服务调用、服务鉴权、服务降级、服务限流、配置管理、调用链跟踪等功能。

7.2.1.2.3 大数据基础平台

要求可基于 Hadoop 体系的 MapReduce、HIVE、SPARK 技术提供强大的数据离线批处理能力，支持查询分析秒级响应，无 cache 情况下；百万级查询获取十万级结果并导出耗时小于 5ms；亿级数据检索并导出十万级结果耗时小于 1s。要求提供 BI 账号服务，可多维分析和报表展现，可快速实现可视化分析报表上线，可以通过拖拽式自服务操作进行交互式分析，快速获得分析结果。

大数据基础平台处理套件要求能够支持 GB、TB、PB 级的大数据处理场景，包括但不限于以下场景：

（1）数据仓库建设

大数据处理套件能够完整覆盖数据抽取、转换、加载、建模、分析、报表呈现、数据治理等数仓建设环节，用户可借助大数据套件快速建设 TB 到 PB 级的数据仓库和数据集市，搭建专属的大数据应用。

（2）实时流式数据处理

用户可基于大数据基础平台套件快速开发本行业在实时流式场景下的大数据处理、分析的应用程序，以实现对实时业务的风险监控与告警，以占据大数据时代的优势地位。

（3）离线数据处理

大数据基础平台套件基于 Hadoop 体系的 MapReduce、HIVE、SPARK 技术向用户提供的强大的数据离线批处理能力，用户可以便捷的使用大数据套件对数据进行抽取、转换、加载等离线数据处理加工。

（4）数据分析与探索挖掘

通过大数据基础平台处理套件所提供的强大数据分析与探索挖掘能力，用户可快速对 PB 级规模下的大数据进行可视化的数据分析探索。

本次政务云提供以下的大数据套件服务内容:

序号	服务目录	服务规格
1	计算资源	定制化服务(2 核/单位）
2		定制化服务(4G 内存/单位）
3	存储资源	定制化服务（1T 存储/单位）
4	BI 账号	提供多维分析和报表展现，快速部署一套数据可视化分析报表，通过拖拽式自服务操作进行交互式分析，快速获得分析结果。

7.2.1.2.3 容器服务

容器服务要求基于原生 kubernetes 提供以容器为核心的、高度可扩展的高性能容器管理服务，为容器化的应用提供高效部署、资源调度、服务发现和动态伸缩等一系列完整功能，解决开发、测试及运维过程的环境一致性问题，提高大规模容器集群管理的便捷性，提高效率。

7.2.1.2.4 灾备国密加密服务

在本地（同城）备份服务和异地备份服务的基础上，提供灾备的国密加密服务，要求兼容类型二服务。

7.2.1.3 软件服务

提供操作系统、数据库、中间件等服务。

- 操作系统包括但不限于：CentOS、中标麒麟、银河麒麟、统信、微软；
- 数据库要求兼容类型二服务，提供包括但不限于：达梦数据库、神通数据库、金仓数据库、瀚高数据库、南大通用数据库、海量数据库、优炫数据库；
- 中间件包括但不限于：金蝶天燕、东方通中间件、宝兰德中间件、中创中间件、普元中间件、TAS 中间件。

7.2.2 类型二服务

7.2.2.1ARM 架构虚拟主机服务

要求提供 ARM 架构虚拟主机服务，要求支持以下能力：

1、支持多种类型云硬盘供选择

2、支持网络自定义，自由划分子网、设置网络访问策略

3、提供公共镜像能力和私有镜像服务，免安装快速部署操作系统与软件

4、提供 VNC 控制台、远程终端和 API 等多种管理方式

5、支持用户申请时指定实例登录方式，虚拟机实例支持多种登陆方式（密码、证书），密码防暴力破解，满足用户的登陆安全需求。

6、支持云硬盘备份，在磁盘故障或数据错误时可快速恢复，使数据更加安全可靠；

7.2.2.2 裸金属服务

要求提供裸金属服务（ARM、MIPS 架构）,可提供以下配置选择：

2 路 48 核，CPU 主频≥2.6GHz，内存≥256G,硬盘≥2*480G SATA SSD, RAID 卡，2 张万兆网卡

2 路 48 核，CPU 主频≥2.6GHz，内存≥256G,硬盘≥3*4T+960GB, RAID 卡，2 张 4 端口万兆网卡

2 路 32 核，CPU 主频≥2.6GHz，内存≥256G,硬盘≥3*4T+960GB, RAID 卡，2 张 4 端口万兆网卡

4 路 4 核，CPU 主频≥1.45GHz，内存≥64G，硬盘≥6TB SATA

1 路 64 核，CPU 主频≥2.2GHz，内存≥64G，硬盘≥4TB*4+240GB SATA

1 路 8 核，CPU 主频≥2.0GHz，内存≥64G，硬盘≥4TB+960GB*2 SATA

1 路 16 核，CPU 主频≥1.6GHz，内存≥64G，硬盘≥8TB+250GB SATA HDD/M.2 SSD

1 路 16 核，CPU 主频≥2.0GHz，内存≥64G，硬盘≥1TB*4 SATA

7.2.2.3GPU 资源服务

要求提供虚拟主机和裸金属服务可选 GPU 显卡服务（仅支持飞腾芯片）。技术要求如下：

人工智能卡中每颗芯片理论峰值(int8)≥128TOPS,单颗芯片≥16GB 内存容量，芯片内存位宽≥256-bit,支持内存 ECC 功能，支持低比特网络模型和量化(int16, int8, int4),芯片内存带宽上限≥100GB/s。

7.2.3 类型三服务

7.2.3.1 安全服务

7.2.3.1.1 基础安全服务

中标供应商建设的政务云平台必须满足信息系统安全等级保护三级要求，即公安部《信息安全等级保护管理办法》第三级安全保护能力。同时承诺在本项目服务期内，由具备国家等级保护测评资质的单位完成等保三级测评，并提供测评单位出具的评测报告和地市级及以上公安部门出具备案证明。

7.2.3.1.2 租户安全服务

为全面提高政务云的信息安全管理水平和控制能力，适应并符合今后不断发展变化的业务新需求，同时遵循国家信息安全等级保护政策法规标准，要求建立一整套适合云平台租户的网络安全保障体系，在政务云机房内部搭建独立的云安全管理平台（安全资源池），包括硬件和软件，实现对租户的安全自助服务，以及安全合规和安全责任的划分。

7.2.3.1.2.1 云主机安全

为租户提供云主机安全组件，具备虚拟化主机安全轻代理防护能力。集成防病毒、主机防火墙、主机入侵防御（虚拟补丁）、虚拟化加固、主机加固、Webshell 检测功能。同一租户，1 套含 5 个实例数。

云主机安全组件提供不少于 3 种病毒查杀引擎，可根据不同虚拟化环境和查杀要求灵活开启与关闭；同时产品应支持利用 CPU 虚拟化技术提升系统的安全防护能力。

客户端采用轻量级 Agent 部署，客户端支持对 windows 类、linux 类；物理服务器、虚拟服务器、桌面云部署模式。为方便统一管理，要求虚拟化主机防护软件具有高度兼容性，应至少支持国内主流虚拟化厂商平台，并能够采用一个管理控制中心进行统一管理。

7.2.3.1.2.2 云防火墙

为租户提供云防火墙组件，提供防火墙+入侵防御安全能力。同一租户，1 个许可含 200Mbps 防护能力。

支持基于源安全域、目的安全域、源用户、源地址、源地区、目的地址、目的地区、服务、应用、隧道、时间、VLAN 等多种方式进行访问控制，并支持地理区域对象的导入以及重复策略的检查。

支持网络漏洞防护功能，同时将漏洞防护特征库分类，至少包括缓冲区溢出、跨站脚本、拒绝服务、恶意扫描、SQL 注入、WEB 攻击等六种分类；漏洞防护支持记录日志、阻断、放行、重置等执行动作,可批量设置针对某一分类或全部攻击签名的执行动作；支持基于 FTP、HTTP、IMAP、OTHER_APP、POP3、SMB、SMTP 等应用协议的漏洞防护。

支持在设备漏洞防护特征库直接查阅攻击的名称、CVEID、CNNVDID、严重性、影响的平台、类型、描述等详细信息。

7.2.3.1.2.3Web 应用防护

为租户提供 Web 应用防护组件,提供虚拟化 Web 防篡改、Web 应用安全防护能力。同一租户，1 个许可含 200Mbps 应用安全防护能力。

要求能提供应用防护及防篡改功能。

应用防护：

1、支持反向代理模式部署 WAF 应用防护组件，当 WAF 配置成观察模式之后，只会对攻击进行检测，不会进行阻断、拦截。

2、支持对命令执行、木马后门、DoS 攻击、SQL 注入、信息泄露、安全绕过、漏洞扫描、目录遍历、缓冲溢出、请求访问、跨站脚本的攻击防护。

3、支持定义多条匹配规则实现 CC 防护，匹配方式需至少支持 严格匹配 和 模糊匹配；支持 检测行为的阻断、系统提示功能，支持验证码校验；支持查看当前命中 CC 攻击规则的 IP；支持查看 CC 攻击的源 IP、攻击次数、开始时间、结束时间信息。

防篡改：

1、同时支持防护模式和监控模式两种模式的防篡改模式。

2、系统支持在断线情况下对网页文件目录的防护功能。

3、应支持文件多线程同步，并可以设置文件空闲同步时间周期、发布时间周期等设置。

7.2.3.1.2.4 堡垒机

为租户提供堡垒机组件,提供运维安全管理与审计系统（堡垒机）安全能力。同一租户，1 个许可含 20 个实例数。

支持 SSH、RDP、VNC、Telnet、FTP 等协议。支持 RDP、SSH、VNC 协议类型主机的文件上传和下载，并进行审计。

命令权限控制动作包含拒绝执行、允许执行、告警、动态授权和断开；堡垒机本身预制主机和网络设备的基本命令，用户可根据特定场景需要进行自定义命令。

支持从一条命令定位到用户的操作过程；回放过程支持暂停和加速播放操作。

7.2.3.1.2.5 数据库审计

为租户提供数据库审计组件,提供数据库审计能力。1 个许可含 1 个可管理数据库实例，单套数据库审计服务能力≤200Mbps。

支持数据库：Oracle、SQL-Server、DB2、Informix、Sybase、MySQL、PostgreSQL、达梦、人大金仓 kingbase、南大通用 Gbase、华为 GaussDB 等数据库的审计，支持后关系型数据库 Cache 的审计。

支持 Telnet、pop3、smtp、nfs 协议审计，针对 FTP 协议，txt 文件传输可对其内容进行审计。

全面支持后关系型数据库 Cache 的集成工具 Terminal、Portal、Studio、Sqlmanager、MedTrak 工具的审计，其中 Portal 能审计到 Sql 语句、查询 Global、返回结果，Terminal 能审计到 M 语句和返回结果。

7.2.3.1.2.6 日志审计

为租户提供日志审计组件,提供统一的日志审计及日志管理功能。同一租户，1 个许可含 10 个实例数。

可为云租户提供所有安全组件的统一日志管理功能，可展示日志概览及各组件的日志情况，无需登录具体的安全组件去查看。

支持按天展示最近发生的所有攻击事件、攻击的详细信息，并能直接单点登录到安全设备上，进行安全策略的配置。

7.2.3.1.2.7 态势感知

为租户提供态势感知组件,提供云安全威胁感知能力。一个服务含 1 个实例数。

云安全管理平台能够提供云安全态势感知服务，采集各类云安全数据信息，形成包括攻击地图、威胁类型及来源、安全组件防护效果、攻击行为趋势、云中站点受威胁等全面的安全态势呈现。

7.2.3.2 密码资源池服务

密码资源池包含密码资源层、密码支撑层、密码服务层、中间件层、密码应用层，依托国产商用密码算法的密码应用体系，利用云计算技术，为部署在电子政务外网的政务信息系统提供密码应用支撑服务。

1、密码资源层提供底层基础设施，即云服务器密码机、服务器密码机、标识服务器密码机、时间戳服务器、智能密码钥匙、SSL VPN、IPSec VPN 等专业设备，通过把虚拟化技术和云管理技术应用在设备集群上，形成集成化的密码资源池。

2、密码支撑层是基于密码资源层中的密码基础设施，把面向应用场景的密码功能集合在一起，打包成易部署、易使用的虚拟机模板、微服务模板软件，在云中以虚拟机实例、微服务实例、软件中间件的形态提供服务。

3、密码服务层是经过功能封装的各项服务，可为政务信息系统提供多种密码应用支撑，主要由密码服务 API 组成，各项密码服务的 API 技术需符合商用密码行业标准。

4、中间件层提供跨平台密码应用，基于底层密码应用支撑服务，封装各类通用的服务接口，制定相应的规范，满足业务应用调用密码服务需求；中间件应支持多种操作系统运行环境。

5、密码应用层是密码应用范围的统称，包括用户层安全密码应用、网络与接入安全密码应用、平台及密码应用、安全管理密码应用四个方面：

1） 用户层安全密码应用：主要包括两种应用场景，即接入单位用户终端安全密码应用和移动终端密码应用；

2） 网络与接入安全密码应用：主要用于实现边界的传输与隔离、身份识别，是进入政务云平台计算环境的第一道门户，主要从网络传输安全、网络可信接入、访问控制、身份认证等控制点进行密码应用；

3） 平台及密码应用：主要包括政务云平台、大数据中心及政务应用三大部分，三大部分涵盖数字政府建设的核心场景，是密码应用的重点；

4） 安全管理密码应用：主要满足管理人员在进行操作时，通过身份认证、授权管理、权限控制、数据远程传输安全及密码合规性管理等方面实现在管理、运营和运维过程中的全过程安全。

7.2.3.2.1 基础支撑能力

7.2.3.2.1.1 密钥管理服务

1、服务描述

密钥管理服务是根据密码接入规范和标准管理协议，为政务信息系统提供密钥生成、存储、更新、备份恢复、销毁、标识密钥全生命周期管理等服务，适用于政务信息系统中需要使用密钥的场景。

2、服务功能说明

1） 密钥生成：通过平台中合规的密码产品生成，包括对称密钥和非对称密钥；

2） 密钥存储：安全存储在平台合规的密码产品或加密存储在密码产品外部，除公钥外，任何密钥都不会以

明文的形式出现在密码产品外；

3） 密钥分发：密钥安全分发，支持通过非对称加密或会话密钥方式分发；

4） 密钥导入：安全导入密钥并安全存储；

5） 密钥导出：指定密钥导出，导出形式为密文；

6） 密钥备份：单条或批量密钥备份，备份形态为密钥密文文件；

7） 密钥恢复：指定密钥文件，将密钥安全恢复到密钥管理服务中；

8） 密钥更新：密钥版本更新；

9） 密钥归档：归档密钥不能使用，但仍存储在密钥管理服务中；

10）密钥销毁：彻底删除密钥管理服务中的密钥；

11）密钥查询：根据密钥信息查询对应密钥。

3、服务配置说明

单个服务能力满足以下配置要求：

1） 并发请求数≥100 次/秒；

2） 密钥存储数量≥10000 个。

7.2.3.2.1.2 加解密服务

1、服务描述

加解密服务是对数据进行加解密、杂凑等密码运算服务，提供信息的机密性、完整性、真实性和不可否认性保护，适用于政务信息系 统中涉及数据加解密的场景。

2、服务功能说明

1） 对称算法加密（SM1、SM4）：提供单条数据加密和批量数据加密接口； 提供指定内部密钥和外送密钥加解密方式；提供多种加密方式：CBC、ECB、CTR、GCM； 提供多种加密填充方式：nopadding、PKCS#5、PKCS#7； 提供消息鉴别码（MAC）计算；

2） 非对称算法加解密（SM2）：提供指定内部密钥和外送密钥加解密方式。

3、服务配置说明

单个服务能力满足以下配置要求：

1） 并发数≥128 个会话连接

2） SM1≥15Mbps

3） SM2 加密≥2300TPS

4） SM2 解密≥1000TPS

5） SM3≥150Mbps

6） SM4≥150Mbps

7.2.3.2.1.3 签名验签服务

1、服务描述

签名验签服务是基于数字签名、验证签名技术，为政务信息系统提供应用级数字签名、验证签名等服务，确保实体身份的真实性、可信性。

2、服务功能说明

1） 提供多种签名验签方式，如 PKCS#1 签名/验证、PKCS#7Attach 和 Dettach 方式的签名/验证；

2） 提供根证书管理功能，包括根证书导入、查看、下载、删除等 功能；

3） 提供用户证书管理，主要包括生成证书请求、证书导入、PFX 密钥导入、证书删除、证书启用/停用等功

能。

3、服务配置说明

单个服务能力满足以下配置要求：

1) 并发数≥128 个会话连接

2) SM2 签名≥2300TPS

3) SM2 验签≥1000TPS

4) SM3≥150Mbps

7.2.3.2.1.4 时间戳服务

1、服务描述

时间戳服务可提供一个能证明数据或电子文件在一个时间点是已经存在的、完整的、可验证的电子凭证，基于数字签名、验证签名技术，按照时间戳标准协议规范，为政务信息系统提供精准、安全和可信时间认证服务。

2、服务功能说明

1) 提供时间戳根证书管理，主要包括根证书的导入、下载、查看、删除等功能；

2) 提供时间戳证书管理，主要包括生成证书请求、证书导入、PFX 密钥导入、证书删除、证书启用/停用等功能；

3) 提供时间戳策略管理，主要包括 RFC 时间戳服务配置，时间戳 OID 列表管理等功能；

4) 提供 NTP 时间源配置。

3、服务配置说明

单个服务能力满足以下配置要求：

1) 时间戳支持并发量≥100 个；

2) 时间戳签发≥80 次/秒；

3) 时间戳验证≥150 次/秒。

7.2.3.2.1.5SSL VPN 安全网关

1、服务描述

SSL VPN 安全网关是基于 SSL/TLS 协议，提供基于国密算法的安全通道建立服务，提供网络实体接入内网的身份鉴别服务；能够为政务网站或应用服务器提供包括 SSL 卸载、TCP 安全通道、UDP 安全通道、4-7 层负载均衡、PKI 就绪、数据优化加速等服务。提供客户端与服务端 VPN 建立的服务，提供服务器认证，客户认证、SSL 链路上的数据完整性和 SSL 链路上的数据保密性等服务。

2、服务功能说明

1) 提供多种服务类型，主要包括 http、https、TCPtoTCP+SSL、TCPtoTCP、UDP、UDP+DTLS 等；

2) 提供单向认证、双向认证；

3) 提供多种 SSL 协议，如 SSLv3、TLSv1、TLSv1.1、TLSv1.2；

4) 提供多种密码算法，如 SM4-SM3、SM2-SM4-SM3、ECC-SM4-SM3、ECDHE-SM4-SM3 等算法。

3、服务配置说明

单个服务能力满足以下配置要求：

1) SSL 加密吞吐率≥500Mbps；

2) SSL 并发连接数≥35000 个；

3) SSL 每秒新建连接数≥1500 个/秒。

7.2.3.2.1.6IPSEC VPN安全网关

1、服务描述

IPSecVPN安全网关是基于IPSec协议，提供基于数字证书的高强度身份认证服务、高强度数据透明隧道加密服务，用于保证通信数据机密性/保密性和完整性，构建安全传输通道，可以有效保护网络资源的安全访问，为用户提供安全接入服务。

2、服务功能说明

1) 提供基于全国产密码算法运算的服务；

2) 提供国密标准IKE协商+国密双证书认证模式；

3) 提供多种安全通道模式，如隧道模式、透明模式、GRE模式等。

3、服务配置说明

单个服务能力满足以下配置要求：

1) 吞吐率≥500Mbps；

2) 最大并发隧道数≥1000。

7.2.3.2.1.7 服务器密码机

1、服务描述

1) 服务器密码机（物理机硬件设备）

物理机硬件设备。为政务信息系统提供数据加解密、杂凑等密码运算，实现信息的机密性、完整性、真实性和不可否认性保护的独享服务器密码机。

2) 服务器密码机（虚拟机密码机）

为政务信息系统提供数据加解密、杂凑等密码运算服务，实现信息的机密性、完整性、真实性和不可否认性保护的独享服务器密码机。

2、服务功能说明

1) 提供国产密码算法和通用国际密码算法服务：对称算法，支持国产 SM1/SM4/SM7/ZUC 算法，支持国际 DES/AES 算法；摘要算法，支持国产 SM3 和通用 MD5/SHA1/SHA256/SHA384/SHA512等算法；非对称算法，支持国产SM2/SM9和通用RSA(1024-4096)算法，支持国际 ECC 椭圆曲线算法；

2) 提供高质量密钥生成服务，提供安全合规的密码算法；

3) 提供安全的密钥管理服务；

4) 提供标准的API接口，如SDF、JCE、P11等。

3、服务配置说明

单个服务能力满足以下配置要求：

1) 服务器密码机（物理机硬件设备）

a) 并发数≥1024个会话连接；

b) SM1 计算速度≥10Mbps；

c) SM2 签名速度≥20000次/秒；

d) SM2 验签速度≥10000次/秒；

e) SM3 计算速度≥800Mbps；

f) SM4 加解密速度≥800Mbps

2) 服务器密码机（虚拟机密码机）

a) 并发数≥128个会话连接；

b) SM1≥15Mbps；

c) SM2 签名≥2300TPS；

d) SM2 验签≥1000TPS；

e) SM3≥150Mbps；

f) SM4≥150Mbps。

7.2.3.2.1.8 签名验签服务器

1、服务描述

1) 签名验签服务器（物理机硬件设备）

基于数字签名、验证签名技术，为政务信息系统提供数字签名、验证签名功能的独享签名验签服务器。

2) 签名验签服务器（虚拟密码机）

基于数字签名、验证签名技术，为政务信息系统提供数字签名、验证签名功能的独享签名验签服务器。

2、服务功能说明

1) 提供多种签名验签方式，如 PKCS#1 签名/验证、PKCS#7Attach 和 Dettach 方式的签名/验证；

2) 提供多种格式内容的签名验签功能，如消息、文件、条码等格式的签名验签服务；

3) 提供加解密服务，包括对称算法和非对称算法的加解密；

4) 提供杂凑算法计算摘要服务；

5) 提供证书管理功能，包括证书申请、证书导入、证书有效性验证等服务；

6) 提供多 CA 对接服务。

3、服务配置说明

单个服务能力满足以下配置要求：

1) 签名验签服务器（物理机硬件设备）

a) 并发数≥1024 个会话连接

b) SM2 签名速度≥25000 次/秒

c) SM2 验签速度≥10000 次/秒

d) SM3 计算速度≥800Mbps

2) 签名验签服务器（虚拟密码机）

a) 并发数≥128 个会话连接；

b) SM2 签名≥2300TPS

c) SM2 验签≥1000TPS

d) SM3≥150Mbps

7.2.3.2.2 通用支撑能力

7.2.3.2.2.1SM9 标识密钥管理服务

1、服务描述

标识密钥管理服务是根据密码接入规范和标准管理协议，为政务信息系统提供密钥生成、存储、更新、备份恢复、销毁、标识密钥全生命周期管理等服务。

2、服务功能说明

1) SM9 密钥管理；

2) SM9 分片密钥密钥管理；

3) SM2 分片密钥的密钥管理。

3、服务配置说明

提供 API 接口文档及技术支持服务，配合应用开发商完成开发对接工作，单个服务能力满足以下配置要求：

1) 并发请求数≥100 次/秒；

2) SM9 标识管理≥1000000 个

7.2.3.2.2.2SM9 服务器密码机

1、服务描述

1) 服务器密码机（物理机硬件设备）

为政务信息系统提供数据加解密、杂凑等密码运算，实现信息的 机密性、完整性、真实性和不可否认性保护的独享服务器密码机。

2) 服务器密码机（虚拟机密码机）

为政务信息系统提供数据加解密、杂凑等密码运算服务，实现信息的机密性、完整性、真实性和不可否认性保护的独享服务器密码机。

2、服务功能说明

1) SM2 密钥生成；

2) SM9 密钥生成；

3) SM3 算法；

4) SM4 算法；

5) SM2 加解密；

6) SM2 签名验签；

7) SM9 加解密；

8) SM9 签名验签。

3、服务配置说明

单个服务能力满足以下配置要求：

1) 服务器密码机（物理机硬件设备）

a) 并发数≥1024 个会话连接

b) SM1 计算速度≥10Mbps

c) SM2 签名速度≥20000 次/秒

d) SM2 验签速度≥10000 次/秒

e) SM3 计算速度≥800Mbps

f) SM4 加解密速度≥800Mbps

g) SM9 密钥生成≥10000 次/秒

2) 服务器密码机（虚拟机密码机）

a) 并发数≥128 个会话连接

b) SM1 计算速度≥10M/s

c) SM2 签名速度≥2000 次/秒

d) SM2 验签速度≥1000 次/秒

e) SM9 验签速度≥1000 次/秒

f) SM3 计算速度≥80Mbps

g) SM4 加解密速度≥60Mbps

h) SM9 签名速度≥2000 次/秒

7.2.3.2.2.3 数据库透明加密服务

1、服务描述

数据库透明加密服务是基于数据库（MySQL、PostgreSQL、达梦、金仓等）提供的原生 TDE 接口能力，对数据库的库表进行加密及安全加固，实现对数据库文件、表空间的加密存储。

2、服务功能说明

1) 预防存储层明文泄密

硬件设备、备份磁盘丢失，数据文件、备份文件的拷贝，外部黑客拖库。

2) 业务透明

数据在写入磁盘之前进行加密，从磁盘读入内存时进行解密，无需更改任何应用程序，对业务透明。

3) 安全合规

支持 SM4 对称算法，独立密钥管理，满足合规要求。

3、服务配置说明

单个服务能力满足以下配置要求：

1) 数据库加解密速率≥60Mbps；

2) 数据库操作性能损耗≤20%。

7.2.3.2.2.4 数据库字段级加密服务

1、服务描述

通过数据库加密技术，对数据库文件、表空间、数据库字段级进行库外加密及安全加固，满足数据存储机密性及完整性要求；支持关系型及非关系型数据库(Mysql、PostgreSQL、Mongodb、Elasticsearch、Oracle、SQL Server、达梦、人大金仓、南大通用 GBase、华为 GaussDB 等数据库)。

2、服务配置说明

单个服务能力满足以下配置要求：

1) SM4 的加密性能在正常场景中能达到 80Mbps；

2) 数据库操作性能损耗≤20%；

3) 单服务节点(CPU14C28T)加密性能≥10 万 QPS。

7.2.3.2.2.5 文件加密服务

1、服务描述

对非结构化文件提供加密服务，保障用户数据安全。

2、服务配置说明

单个服务能力满足以下配置要求：

1) 要求文件读写操作性能损耗≤20%；

2) 文件加密速率≥400Mbps。

7.2.3.2.2.6 数据静态脱敏服务

1、服务描述

支持自定义敏感数据特征和脱敏算法，对敏感数据识别，适用于数据离线共享分发脱敏，支持结构化数据与非结构化数据。

2、服务配置说明

静态脱敏性能≥25GB/小时。

7.2.3.2.2.7 数据动态脱敏服务

1、服务描述

支持自定义敏感数据特征和脱敏算法，对敏感数据识别，适用于 API 接口、运维等敏感业务场景，支持结构化数据。

2、服务配置说明

动态脱敏性能≥15000 条 SQL/秒。

7.2.3.2.3 增值服务

7.2.3.2.3.1 证书管理服务

1、 服务描述

证书管理服务，是指为电子签名相关各方提供真实性、可靠性验证的活动。根据我国颁布的《电子认证服务管理办法》，电子认证服务提供者，是指为需要第三方认证的电子签名提供认证服务的机构。

证书管理服务可以解决 GB/T39786-2021《信息安全技术信息系统密码应用基本要求》中对身份真实性、不可否认性方面的需求，也满足《中华人民共和国电子签名法》要求。

证书由合规的第三方 CA 认证机构签发数字证书，为租户设备、机构、个人提供网络身份认证、电子签名服务，以保障其身份真实性，电子签名合法性。

2、 服务功能说明

1) 证书申请服务

对机构单位和个人的申请资料进行审核确认，按照国家认证的证书发放机构要求进行证书申请材料的整理和确认。在线提交资料进行办理申请。

2) 证书办理服务

对符合条件和通过资料审核的机构单位或个人，在线办理进行证书办理。

3) 证书变更服务

对用户变更资料进行审核、整理和确认。在线申请办理变更业务进行证书申请办理变更手续。

3、 证书管理服务

1) 证书注销

在单位或个人的数字证书遗失、持数字证书人员岗位变更或需数字证书内容变更的情况，为以防止信息外泄，提供办理证书注销业务工作资料审核、申请和办理服务。

2) 证书解锁

在证书因各种情况，如信息外泄、资料变更等情况，对已锁定的证书使用单位或个人，提供办理证书解锁业务工作资料审核、申请和办理服务。

3) 证书遗失补办

当单位或个人持有的数字证书丢失时，提供办理证书遗失补办业务工作资料审核、申请和办理服务。

4) 证书有效期更新

当用户发现持有的数字证书有效期即将到期时，提供办理数字证书有效期的延长业务操作指导或办理，及时延长证书有效期保障用户对证书的正常使用。

4、 服务配置说明

证书管理服务提供机构证书、个人证书、服务器证书三类数字证书的管理服务。

1) 机构证书服务

采用国家认可的权威第三方 CA 机构证书，提供验证国密证书签发和管理服务，应用于政府部门标识真实身份。

2） 个人证书服务

采用国家认可的权威第三方 CA 机构证书，提供国密证书签发和管理服务，应用于个人用户标识真实身份。

3） 服务器证书服务

采用国家认可的权威第三方 CA 机构证书，提供国密证书签发和管理服务，应用于政务信息系统之间标识真实身份。

7.2.3.2.3.2 智能密码钥匙服务

1、 服务描述

为政务信息系统提供密码运算、密钥管理功能的终端密码设备，应至少支持：USB、SD、Dock、Lighting、Bluetooth、NFC、音码、WiFi、ISO7816、ISO14443 接口。

2、 服务功能说明

1） 签名验证

支持 SM2 密钥对生成并进行签名验证运算。

2） Hash 运算

支持 SM3 算法，通过 Hash 运算实现完整性校验。

3） 身份鉴别

通过智能密码钥匙+用户口令进行身份认证，保证用户的合法性；

4） 数据加密

应用于数据存储、数据处理、数据传输场景中，对敏感信息数据、文件数据的加解密保护。

5） PKI 应用

支持数字证书存储、管理，支持公私钥的签名验证运算。

3、 服务配置说明

单个服务能力满足以下配置要求：

1） SM2 密钥生成时间≤5 秒；

2） SM2 数字签名时间≤500 毫秒；

3） SM3 速度≥2Kbps。

7.2.3.2.3.3 国密浏览器服务

1、 服务描述

国密浏览器服务是提供支持 SM2、SM3、SM4 等国密算法的浏览器，适用于政务信息系统需要安全访问页面的场景。

2、 服务功能说明

1） 跨平台控件兼容

支持在 Blink 内核模式下调用 IE 控件，在保障安全性的同时加强浏览客户端的易用性，而用户原有 IE 控件无需做任何修改，即可将原有 B/S 应用平滑移植到国密浏览器上。

对于特定的应用，可采用指定 IE 内核版本的方式，使用户的应用、IE 控件运行在指定的 IE 内核版本下，而无需关注用户安装的 IE 浏览器版本，以进一步提高用户使用环境的稳定性。

2） 国产算法支持

支持基于 SM2/SM3/SM4 密码算法套件的单双向 SSL 协议，并支持使用基于 SM2 算法的 USBKey 登录电子政务页面。

在 IE 内核与 Chrome 内核下，均支持国产密码算法与国密 SSL 协议。

3） 证书管理

支持国家密码管理局的 SM2 证书链的管理，支持根证书的存储、用户证书的查看、证书链有效性的验证、证书更新提醒等功能。

4） U 盾管理

国密安全浏览器支持 U 盾管理，支持调用国密 SKF 库等标准接口，实现不同厂家 U 盾的枚举、PIN 码修改、U 盾管理等功能。

5） 多操作系统平台

除了全面支持 Windows 系列操作系统，支持国产操作系统、Linux 平台。

6） 自动升级服务

通过搭建后台管理服务器，支持自动升级服务，采用增量升级模式，只升级修改过的国密安全浏览客户端文件，其中控件、USBKey 驱动可独立升级，减轻升级服务器带宽负担。其中升级模式支持提示用户升级、后台自动升级、强制升级三种模式，无公开浏览器升级之忧。

3、 服务配置说明

单个服务能力满足以下配置要求：

基于 SSL 隧道，吞吐率≥9Mbps

7.2.3.2.3.4 终端密码模块服务

1、 服务描述

采用密钥分割技术，为终端提供符合国密二级密码模块要求的密码应用“软卡”，以软件 SDK 方式为移动端提供认证、加密、通信等安全防护服务。

2、 服务功能说明

1） 密码运算：支持国密 SM2 加解密算法、SM3 哈希算法、SM4 对称加解密算法；

2） 密钥存储：支持对称密钥和非对称密钥的存储。

3、 服务配置说明

单个服务能力满足以下配置要求：

1） SM2 速度≥20 次/秒；

2） SM4 速度≥100Mbps

7.2.3.2.3.5 密码支撑服务

密码支撑服务是指通过人工方式对业务系统密码应用安全性进行评估，找出问题差距，并提出整改建议，整体对密码应用改造提供整改服务。

7.2.4 类型四服务

为政务云提供运行服务，包括对整体资源的使用率实时预警，及时响应扩容；实时对用户使用问题进行跟踪，提高用户感知；保证平台平稳运行。

7.2.4.1 政务云运营服务台

提供 7*24 运营响应服务,包含电话、IM 在线、邮件等方式。服务台工作内容主要是问题管理、知识库管理、服务质量报告、SLA 跟踪督办等。

7.2.4.2IaaS 平台运营

为 IaaS 层软硬件及其配套应用提供运营服务。包括 IaaS 资源分配管理服务、IaaS 容量管理服务、机房与设备管理服务、服务管理服务、运维管理服务、服务跟进与分析报告服务等。

数据中心网络运营。为东莞市政务云平台内部网络提供运营管理服务，包括为政务云平台服务使用方提供网络技术支撑服务，提供网络需求管理服务（含策略开通管理）、故障管理服务、技术支撑服务、供应商管理服务等。

软件运营。为服务器操作系统、数据库系统、中间件等各类软件提供运营服务，包括技术支撑服务和服务管理服务。

硬件托管服务运营。为数据中心机房托管设备提供运营服务，包括托管需求管理服务、设备台账管理服务、供应商管理服务等。

7.2.4.3PaaS 平台运营

PaaS 层软件运营。为 PaaS 软件（不包括大数据基础平台）提供运营服务，包括 PaaS 资源分配管理服务、资源容量管理服务、服务管理服务、风险管理服务、交付验收管理服务、技术支撑服务等。

大数据基础平台运营。为大数据基础平台提供运营服务，包括大数据基础平台资源分配管理服务、容量管理服务、服务管理服务、技术支撑服务等。

7.2.4.4 灾备运营

为数据备份和容灾服务提供运营管理服务，包括灾备需求管理服务、灾备运维管理服务、服务管理服务、灾备重保服务和服务跟进与分析报告服务。

7.2.4.5 其他运营服务

政务云测试区运营。为测试区提供运营管理服务，包含 IaaS 和 PaaS 层相关的需求管理、资源管理及相关技术支撑工作。

运营分析服务。通过对东莞市政务云平台的建设、运维和运营各阶段工作开展定期或专项的分析服务，提升平台运营水平，包括云平台服务需求收集及其有效性分析、资源发放效率分析、资源低负载及伸缩容服务使用报告、动态扩缩容可行性分析等。

8 运维服务与应急保障要求

中标供应商作为政务云数据中心机房中相关软硬件资产的主要负责主体，主要职责包括：

（一）根据采购人出具的 IaaS 和 PaaS 资源需求函提交建设方案，并根据采购人的方案确认意见在要求时限内完成政务云平台软硬件资产及其承载服务的扩容建设和交付，向采购人移交建设和扩容的验收文档，进行技术讲解；

（二）负责机房的进出登记和操作监视陪同；

（三）负责机房和设施设备的物理安全；

（四）负责机房动环系统的运行维护，包括供配电系统、UPS 系统、空调通风系统、综合监控系统、机柜和综合布线系统、消防系统、接地及防雷系统、门禁系统等；

（五）负责机房中中标供应商所投入政务云设施设备的维护服务，包括服务器、存储、网络交换机、防火墙、VPN 设备、负载均衡等硬件及设备所提供的功能；

（六）负责包含的政务云设备、网络的业务运营支撑，包括网络应用服务、网络配置等；

（七）负责机房中中标供应商所采购政务云平台灾备应用的运行维护，包括灾备应用系统、灾备配置和备份任务；

（八）负责提供机房及其所投入软硬件资产和服务的 7*24 小时的监控告警、响应值班和事项处理服务；

（九）负责主机托管机柜及其电源和柜顶交换机的运行维护；

（十）负责根据采购人的需求，对建设的 IaaS、PaaS 资源进行发放、调整和回收操作；

（十一）负责对建设的软硬件资产、平台及其提供的服务进行运行维护；

（十二）配合执行重要保障工作，开展各类演练工作；

（十三）服从采购人的运维管理，接受采购人的工作安排和考核。

8.1 运维服务

（1）服务团队要求：中标供应商需提供素质高、专业性强、经验丰富、稳定的运维团队，主要负责整个云平台的软硬件和网络运维；中标供应商需建设有严格的、有组织有纪律的管理运维流程（参考 ITILv3 标准），并指派 1-2 名专职接口人，团队需要 7*24 在岗及时响应故障请求，负责云平台的故障受理、处理、跟踪、结果汇报工作。

（2）服务时间要求：提供 7*24 不间断技术服务支持时间。

（3）故障响应时间要求：提供机房运维保障人员和运维接口人员，确保 7*24 小时电话通畅，机房运维需保证 7*24 小时维护；运维接口人员 7*24 小时响应故障、需求； 如人员更换，须提前做好交接确认，并邮件及书面通告。

（4）中标供应商须具备完善的备件库。

（5）为确保政府信息化应用系统和信息的安全保密，供应商需分别与采购人以及相关运维人员签署保密协议。此外，供应商还应定期对运维工作人员进行技能培训、安全保密教育和培训。供应商所配备的所有运维人员应能通过用户方指定的涉密工作资格培训。

（6）中标供应商需要在按资源租赁服务合同要求提供指定的资源服务外，还需要额外提供所有云服务合同中各项资源的 5%预留为应急资源，此部分资源按实际使用量收费。

8.2 应急保障

当云平台系统或基础设施环境发生突然的、影响面广、涉及范围大的紧急故障，对系统数据安全与服务质量造成严重后果的系统或设备事故，将按应急响应流程进行处置。按事故的影响范围的考虑，分别按以下 7 个方面的设施及系统采取相应的应急保障措施：

（1）机房电力故障应急保障

机房电力系统若出现紧急故障，中标供应商提供不低于以下内容的保障：

电力供应：两路一类市电由两个不同的变电站引入机楼，每个机架均由不同的 UPS 引入两路供电。

发电机：并且配备了变压器和柴油发电机，保证电力的供应。

UPS 能力：采用 N+1 的冗余备份 UPS 系统，所有设备机架供电应由双回路电源供电。

电池能力：UPS 电池在满负载情况下可支撑 15 分钟。机柜供电：双路不间断供电。

电力应急主要是由两个变电站的市电引入到机楼，并且转换为 UPS 给每个机柜供电，保证了当其中一路市电中断时，能够无缝切换到另外一路市电给机柜的设备供电。

若出现两路市电均中断的情况，机柜供电马上能够无缝切换到机房内的 UPS 电源供电，整个过程不会对设备正常运行造成影响。

（2）光纤链路故障应急保障

中标供应商机房连接到电子政务外网相应区域的核心层，使用 8 芯裸光纤和万兆网络进行互联，与现有电子政务外网统一组网。

光纤链路若当其中一对（2 芯）光纤故障时，通过此线路的数据包会短暂的丢包，但很快经过网络的冗余路由，网络恢复。

若光纤链路故障，可以启用备用的光纤。

（3）云平台网络层故障应急保障

云平台的核心/汇聚层交换机与接入层交换机通过虚拟交换单元技术实现网络虚拟化。2 台核心/汇聚交换机通过万兆光纤链路互联，形成双机虚拟化。接入层交换机之间通过万兆光纤链路互联，形成双机虚拟化，提供设备冗余、链路冗余、负载均衡等应急处理能力。

云平台内计算节点服务器的每个网络至少提供两个网卡进行，分别连接到不同的汇聚交换设备，若服务器的其中

一网卡出现断开，网络不会中断。

（4）光纤交换机故障应急保障

充分考虑到未来云平台承载大量的虚拟机以及数据库系统，SAN 存储网络的存储交换机采用冗余设计，防止单个交换机失效，交换机和 SAN 存储交叉互联，起到链路冗余的作用。

（5）云控制器故障应急保障

云中部署云控制器的双机热备模式，并且云控制服务器出现故障时，虚拟机的访问和管理并不受影响。

（6）同城应急灾备链路保障

云平台通过光纤连接到同城灾备中心，可以实现生产网络数据的备份；为保证用户数据的安全性，根据各使用单位的业务需求，提供数据同城异地备份服务。

（7）存储故障应急保障

存储系统采用多控制器、多路径的设计方式。不同控制器通过多条链路连接到存储交换机上，保障存储网络不存在任何单点故障。同时在本地提供备份存储节点，当生产存储节点出现问题时，要求备份存储节点立即接管业务确保不会造成业务数据丢失。

8.3 应急演练

中标供应商需建立应急预案机制，每年至少组织一次应急演练。每年需制定或修订应急演练计划，并与采购人及各使用单位充分协商，充分听取采购人及各使用单位意见。按照采购人要求，定期执行应急演练计划，并且至少在演练开始前一周之前通知采购人和各使用单位。记录和核查应急演练结果，并根据需要修正应急响应计划。同时，向采购人和使用单位提供演练记录、演练总结报告等。

9 服务考核要求

9.1 服务质量控制指标

1.中标供应商保证云平台基础云计算资源年度可用性为 99.95%。（计算公式=1-{应用系统年度不可用总历时（分）/年度总时长（分）*系统总数*100%}），经采购人同意的计划性维护以及不可抗力因素导致的故障时间不统计。

2.中标供应商保证云网络整体连通率为 99.99%。计算公式=1-{年度故障总历时（分）/年度总时长（分）*网络线路总数*100%}），经采购人同意的计划性维护以及不可抗力因素导致的故障时间不统计。

3.供应商按 GB/T22239-2008《信息安全技术信息系统安全等级保护基本要求》通过第三级安全认证,做好云平台的安全防护工作。

9.2 服务质量保障措施

1.客服服务：中标供应商建立客服中心作为云平台服务统一接口，受理各种服务请求，并提供 7*8 小时的客服服务，服务内容包括：

（1）业务咨询。包括但不限于云资源申请流程咨询、业务受理进度、云资源使用咨询、其他咨询等；

（2）业务受理。包括但不限于资源使用情况监控、安全问题处理、系统上线处理、服务器回收处理、资源变更处理、机房访问处理、运维进入云平台测试处理等；

（3）业务开通。包括但不限于云平台资源分配、端口开通、VPN 账号开通续期等；

（4）业务售后。包括但不限于投诉建议处理、客户回访，以及通过短信平台发布云平台重大事项等。

2. 技术服务：

（1）中标供应商建立运营支撑团队，提供 7*24 小时的技术支持服务；

（2）中标供应商在 5*8 小时服务时段内，按采购人提交需求提供下列服务，并规定服务开通时限。

序号	服务类	服务项	服务可用时段	服务响应时间	服务完成时间

序号	服务类	服务项	服务可用时段	服务响应时间	服务完成时间
1	业务开通	云主机	5*8 小时	30 分钟	8 小时
2		云存储	5*8 小时	30 分钟	8 小时
3		云负载均衡	5*8 小时	30 分钟	8 小时
4	资源扩容	主机扩容	5*8 小时	30 分钟	8 小时
5		备份存储扩容	5*8 小时	30 分钟	8 小时
备注		以上服务时限工作量为每天 10 台云主机以内，特殊类别或定制化的服务需求完成时限由双方协商确定。			

（注：VPN、非互联网类端口开通完成时间应为 8 小时，互联网类端口开通和云主机 C 盘扩容等按实际情况进行）

（3）在采购人（或采购人指定的单位）新建电子政务项目技术评审阶段，中标供应商负责对云平台资源需求进行预审，原则上 3 个工作日内完成。

（4）中标供应商不直接对用户部门信息系统的运维提供支持，在获得用户部门正式授权前，中标供应商无权对系统设备进行任何操作，获得授权后通常限于重启、检查网络端口、登陆服务器等内容。中标供应商不承担由于授权操作而产生的任何责任；

（5）中标供应商提供 7*24 小时云资源监测服务，包括云主机、云存储的可用性和性能参数，网络连通性等。

3．报告提交

（1）中标供应商监控发现用户单位的云主机 CPU、内存以及存储空间出现资源瓶颈时，应及时通知用户单位向主管部门提出升级申请。

（2）中标供应商根据用户单位需求提供云主机性能使用情况报告。

（3）中标供应商每月 10 日前（遇节假日顺延）向各用户单位提供上个月的资源使用月报，对用户单位反馈问题及时回应，尽快解决，不断提升服务水平。

（4）中标供应商每半年、年底向采购人提交服务报告，对服务工作进行总结梳理，提出改进意见建议。

（5）中标供应商受理用户单位书面投诉后，应在 5 个工作日内完成服务诉求，并向用户单位及采购人提供书面形式的处理报告。

9.3 服务管理要求

1．机房管理要求

(1)云平台机房配置齐全，布局合理，干净整洁，消防和报警系统功能完好，各种标识清晰。

(2)机房提供专人 7*24 值班巡查，安防系统运行良好，人员进出记录保存半年以上，监控录像保存三个月以上。

(3)机房必须保证 UPS 电力续航时间在 120 分钟以上（无柴油发电机情况），在市电出现特殊原因中断时应有应急救援机制。

(4)机房物理环境必须落实每日巡查登记制度，记录应真实、准确、及时。

2．安全管理要求

(1)员工上岗前要参加安全培训，签订《保密协议》，签约率达到 100%。

(2)中标供应商按照权限分离原则加强系统管理权限、超级用户权限和信息安全审计权限的管理。技术人员不得获得、保留用户单位的主机和应用系统的权限，不得直接访问和私自保留用户单位数据。

3．故障管理要求

云平台出现的任何故障都定义为事件，事件指的是由于云平台的硬件/软件出现故障（硬件损坏、未知软件的 BUG 等），中标供应商及时处理故障将影响降到最小，且对使用单位的业务系统没有造成实质性的影响，称为事件。

事故指的是中标供应商提供的平台产生的故障或没有及时排除故障/事件（含主观和客观因素，不可抗拒因素除外），导致云平台的业务受影响或对各使用单位的业务或业务系统造成影响，如业务不可访问、数据丢失等，则定义为

事故。

事件/事故责任范围说明：使用单位责任范围为操作系统以上层面含操作系统本身的故障，由使用单位负责，中标供应商需配合解决；中标供应商责任范围包括但不限于机房环境、物理主机、存储设备、网络设备、安全设备、灾备设备、由中标供应商负责提供的光纤链路、虚拟化层、云平台管理软件层以及人为造成的故障等，都属于中标供应商负责的范围。

事故考核工作由采购人根据平台的监控数据及用户反馈等信息进行分析及鉴定，定义事故等级。若经鉴定事故成因在于中标供应商或者中标供应商未能及时处理的，中标供应商需要承担因中标供应商主观或客观因素引发事故所造成的所有直接和间接经济损失。

事故考核及处理规则如下：

事故等级	事故定义	事故处理要求	处罚规则
一级事故	云平台发生故障导致业务系统业务中断、数据丢失。	处理时间要求：远程响应时间<5 分钟；非正常上班时间响应<0.5 小时；正常上班响应时间＜3 分钟；事故解决时间<1 小时	处罚金额包括以下 2 部分： 1、每发生 1 次一级事故，中标供应商必须接受处罚，处罚金额以“业务受影响时长”（以小时为单位）乘以“受影响业务系统的资源年租赁费”，再乘以“事故等级系数”。多个业务系统受影响，则进行累加。具体计算方法为：时长（以小时为单位）*资源年租赁费*事故等级系数（一级事故系数为 3）＝处罚金额（元）。举例：若 A 业务系统所有资源的年租赁费为 8000 元，发生了 1 个小时一级事故，则处罚金额为 1*8000*3=24000 元。 2、系统发生数据丢失或者对业务系统产生实质性影响，造成无法挽回的直接或间接的经济损失（包含名誉损失），经第三方服务监督机构核损后，中标供应商需要赔付所有的损失。
二级事故	云平台故障发生，但对业务运作影响较小；或者由于云平台故障，导致数据丢失，但是可以恢复、不会影响到业务运作的故障，并明确了完成时间的事件或故障。	处理时间要求：远程响应时间<10 分钟；非正常上班时间 响应<0.5 小时；正常上班响应时间＜5 分钟；解决时间<2 小时	每发生 1 次二级事故，中标供应商必须接受处罚，处罚金额以“业务受影响时长”（以小时为单位）乘以“受影响业务系统的资源年租赁费”，再乘以“事故等级系数”。多个业务系统受影响，则进行累加。具体计算方法为：时长（以小时为单位）*资源年租赁费*事故等级系数（二级事故系数为 2）＝处罚金额（元）。举例：若 A 业务系统所有资源的年租赁费为 8000 元，发生了 1 个小时二级事故，则处罚金额为 1*8000*2=16000 元。
三级事故	对业务运行影响微弱，或者不存在影响，同时遵循一般流程可处理的事故。	处理时间要求：远程响应时间<10 分钟；非正常上班时间响应<1 小时；正常上班响应时间＜5 分钟；解决时间根据甲乙双方约定时间。	每发生 1 次三级事故，中标供应商必须接受处罚，处罚金额以“业务受影响时长”（以小时为单位）乘以“受影响业务系统的资源年租赁费”，再乘以“事故等级系数”。多个业务系统受影响，则进行累加。具体计算方法为：时长（以小时为单位）*资源年租赁费*事故等级系数（三级事故系数为 1）＝处罚金额（元）。举例：若 A 业务系统所有资源的年租赁费为 8000 元，发生了 1 个小时三级事故，则处罚金额为 1*8000*1=8000 元。

4．云主机资源回收期限管理

中标供应商在服务期内，必须遵从采购人的考核办法。考核按每季度进行，若中标供应商考核不合格，采购人有权暂停其服务资格，并提出整改要求；中标供应商需按采购人提出的整改要求及期限进行整改，直至满足采购人要求，并经采购人确认后方能恢复提供服务；连续两次考核不合格或拒不整改的，采购人有权要求中标供应商退出服务。

中标供应商必须承诺在服务退出时，需确保使用单位的业务系统平滑迁移至各使用单位指定的新服务平台。若中标供应商不能满足使用单位的迁移要求，视同中标供应商违约。

迁移完成后，中标供应商需对业务系统以及数据进行彻底删除处理，不得保留、复制或拷贝，并保证数据不可恢复；处理方案必须经采购人和各使用单位的书面同意，并在采购人的监督下进行，处理结果需经采购人及各使用单位共同确认方可退出；如果部分数据有保密需求，中标供应商需对该部分数据所使用的硬盘进行销毁处理，以确保数据安全。

9.4 服务考核要求

1．双方签署的服务水平协议(SLA)作为年度服务采购子合同的附件，是服务考核的基本依据。每年年底前双方可对服务内容进行调整，经书面确认后在下一年度执行。

2．采购人按照合同约定的考核周期向用户部门进行满意度调查，满意率是采购人考核中标供应商服务质量的重要依据。中标供应商可协助采购人进行满意度调查工作。

3．中标供应商每月向采购人提交云平台运行月度报告，作为采购人核算服务费用、考核服务质量的依据。

4．中标供应商根据本协议制定考核实施方案，按照合同约定的考核周期组织服务考核，其中年中考核重点是核对服务量，以作为服务费用支付凭证。年终考核重点是年度服务质量水平，是落实服务质量奖罚标准的关键指标。

5．云平台服务质量考核按照以下奖罚标准执行,考核指标体系按百分制进行考核。具体的考核指标体系如下：

一级指标	二级指标	三级指标	指标说明用核算标准
1-1 运维服务质量（50 分）	2-1 服务请求完成情况（15 分）	3-1 日常服务请求完成率（5 分）	日常服务请求 包含业务咨询、技术咨询等咨询类服务。 完成率=已完成服务请求数量/服务请求总数。 完成率以 5%为一个考核区间，100%得满分，以后每降低 5%扣 0.25 分。
		3-2 资源服务请求完成率（10 分）	资源服务请求包含业务开通、资源变更等资源类服务。 完成率=已完成资源服务请求数量/资源服务请求总数。 完成率以 5%为一个考核区间，100%得满分，以后每降低 5%扣 0.5 分。
	2-2 故障响应服务质量（35 分）	3-3 云计算资源年度可用性(10 分)	云计算资源年度可用性≥99.95%。 云计算资源年度可用性=1-（应用系统年度不可用总历时（分）/年度总时长（分）*云平台应用系统总数）*100%。 年度可用性≥99.95%得满分，99.9%≤年度可用性＜99.95%之间得分 5 分；年度可用性＜99.9%之间得 0 分。
		3-4 云计算资源故障次数考核（10 分）	一级故障每发生 1 次扣 1.5 分，二级故障每发生 1 次扣 1 分，三级故障每发生一次扣 0.5 分，直至扣完为止。
		3-5 云计算资源故障解决时间考核（15 分）	云计算资源一级故障解决时间不达标扣 1.5 分；云计算资源二级故障解决时间不达标扣 1 分；云计算资源三级故障解决时间不达标扣 0.5 分，扣完为止。
1-2 运维服务能力(30 分)	2-3 制度落实(10)	3-6 日常运维操作管理（5 分）	安全运维规范，维护审计严格，配置信息备份完整。根据资料完整度扣 1-5 分。
		3-7 按规定输出运行报告（5 分）	按采购人要求输出月报、半年报、年报，每少 1 份扣 0.3 分，扣完为止。
	2-4 机房管理（10 分）	3-8 安全管控（5 分）	机房安全管理严格，安防系统运行良好，人员进出资料完整。根据资料完整度扣 1-5 分。
		3-9 机房巡检完成率（5 分）	完成率=按时完成的巡检次数/应巡检总数。 达标率以 10%为一个考核区间，100%得满分，每降低 10%扣 0.5 分。
	2-5 应急能力提升（5 分）	3-10 应急预案及演练（5 分）	提供故障紧急处理、电源应急保障预案并每年组织两次应急演练，每少 1 次扣 2.5 分，扣完为止。
	2-6 学习培训（5 分）	3-11 培训交流（5 分）	每年至少组织两次一定规模的用户单位培训交流，每少一次扣 2.5 分，直至扣完为止。
1-3 客户满意度(20 分)	2-7 用户单位评价(10 分)	3-12 用户单位整体评价(10 分)	用户单位评价，分值区间为 0-10 分
	2-8 技术能力(4 分)	3-13 事件与问题的处理效果(4 分)	用户单位评价，分值区间为 0-4 分
	2-9 服务态度(3 分)	3-14 工程师和客服人员服务态度评价(3 分)	用户单位评价，分值区间为 0-3 分
	2-10 服务响应时间(3)	3-15 服务响应是否及时(3 分)	用户单位评价，分值区间为 0-3 分
1-4 加减分项，1-1 至 1-4 总得分不超过 100 分）	2-11 运维服务能力-加分指标（6 分）	3-16 当年度获得专利和省级或以上奖项（ISO、守合同等商务型奖励除外）（6 分）	每项专利 2 分，每项国家级奖励 3 分、每项省级奖励 2 分，本项加分最多不超过 6 分
	2-12 客户满意度-加分指标(5 分)	3-17 书面表扬（非云平台故障原因）(5 分)	上级部门或主管部门书面表扬 1 次加 1 分，用户单位书面表扬 1 次加 1 分；中标供应商前往用户现场进行技术支撑（非故障原因）获得用户书面认可 1 次加 0.5 分。
	2-13 客户满意度-扣分指标(5 分)	3-18 书面投诉(5 分)	用户单位书面投诉（加盖公章）1 次扣 1 分，最多不超过 5 分。
	2-14 云平台稳定性加分指标（3 分）	3-19 云平台持续稳定性（3 分）	对云平台当年最长无故障连续时长进行奖励，满 6 个月（自然月）未出现故障加 1 分，连续 12 个月（自然月）未出现故障加 3 分。
	2-15 针对重点应用系统稳定性的考核	3-20 重点应用系统的稳定性（5 分）	采购人指定的重点应用系统出现一次故障扣 0.5 分。
	2-16 针对数据安全的考核（5 分）	3-21 数据安全保障程度（5 分）	经认定，因中标供应商内部管理原因导致云平台个别少部分应用系统发生人为数据破坏事件、云平台数据卷没按计划成功备份、云平台发生误操作导致云主机不能恢复，影响个别少部分应用系统业务数据的恢复，

一级指标	二级指标	三级指标	指标说明用核算标准
			出现一次扣 5 分。

按照以下奖罚标准执行：

总体得分	处罚说明
95 分≤总体得分＜100 分	中标供应商下一年服务考核分数奖励 1 分-5 分，并向中标供应商支付考核期内有效所属类别资源租赁服务总额
90 分≤总体得分＜95 分	向中标供应商支付考核期内有效所属类别资源租赁服务总额
85 分≤总体得分＜90 分	向中标供应商处以扣除考核期内有效所属类别资源租赁服务总额的 a%(待协商）
80 分≤总体得分＜85 分	向中标供应商处以扣除考核期内有效所属类别资源租赁服务总额的 2a%
75 分≤总体得分＜80 分	向中标供应商处以扣除考核期内有效所属类别资源租赁服务总额的 3a%
70 分≤总体得分＜75 分	向中标供应商处以扣除考核期内有效所属类别资源租赁服务总额的 4a%
65 分≤总体得分＜70 分	向中标供应商处以扣除考核期内有效所属类别资源租赁服务总额的 5a%
60 分≤总体得分＜65 分	向中标供应商处以扣除考核期内有效所属类别资源租赁服务总额的 6a%
总体得分＜60 分	向中标供应商处以扣除考核期内有效所属类别资源租赁服务总额的 7a%

10 知识产权

（1）本项目为政务云服务购买，不涉及知识产权。

（2）采购人依本协议及业务订单向中标供应商提供的宣传资料和宣传资料中所包含的创意、设计、图形、图片、文字等以及因本协议产生的作品（包括但不限于任何图案、图像、配音、配乐、文字、专题片语、卡通人物形象、FLASH 片等，无论是否被采购人最终选用），其全部知识产权和/或其它权益全部归采购人所有，未经采购人事先书面许可，中标供应商不得为本协议及业务订单之外的目的自行使用或许可任何第三方使用。

（3）任何一方在本协议项下合作项目前，已申请、创设、取得或以其他方式拥有的技术，包括但不限于专有技术、信息数据等，均归其自身继续所有，不因本协议项下的合作而发生转移；未经对方事先同意，任一方不得擅自使用、复制对方的商标、标志、商业信息、技术及其他资料。

11 客户数据

最终客户存储、上传到本项目约定的 IaaS 或 PaaS 或 SaaS 政务云服务中的数据，或者利用本协议约定的 IaaS 或 PaaS 或 SaaS 政务云服务以分析、分发等任何方式处理的数据，为最终客户的数据，权属归最终客户所有；未经最终客户同意，中标供应商不得接触或者使用、删除、更改最终客户的数据。

12 项目质量保证要求

（1）中标供应商在云平台运维过程中，应有运维工作方案，方案明确运维流程标准，并进行详细的流程说明，确保运维活动遵循标准的方法、程序和规则，且有记录可追踪，降低运维活动对本项目服务质量的负面影响。

（2）中标供应商在云平台运维过程中，应建立管理规范，包括机房管理、 资产管理、设备管理、介质管理、系统运维管理、灾备管理、用户账号及权限管理和风险管理。

（3）中标供应商在政务信息系统备份设备以及备份系统运行维护中，应建立服务规范，包括备份系统运行维护技术服务规范、基本流程的服务规范。

（4）中标供应商应具备云平台应急事件处理能力，对云平台应急保障的总体组织架构进行划分，并明确各岗位相应的职责。同时应制定标准的应急事件响应、处置流程以及应急预案演练流程。

（5）中标供应商应具备规范的云平台系统保障体系，确保云平台安全、稳定运行。保障体系包括实施运维人员 24 小时值班制度，协调处理故障，问题的快速响应解决以及故障报告分析等。

（6）在不影响中标供应商履行本合同项下义务的情况下，采购人有权在工作时间内对中标供应商履约情况进行检查，以保证供应商项目的任何部分均符合本合同的要求。中标供应商须对此项检查予以协助。

（7）中标供应商应根据质量检查的结果对项目质量问题及时进行整改处理，同时对质量管理的运行情况进行总结与分析，对成功的经验加以肯定，并予以标准化，对失败的教训进行总结，引起重视。对未能及时处理解决的问题，

需将其作为下一次管理循环的质量改进目标。项目质量问题解决完成后，需对实施效果进行评估和记录。若采取的整改措施未达到预期效果，应重新制定解决措施， 直至达到预期效果。

（8）采购人有材料证明中标供应商服务实施过程中与本协议所规定的或其他相关部门所规定的质量或安全要求严重不符时， 采购人有权立即通知中标供应商，中标供应商应按照要求进行整改。若中标供应商在收到采购人书面通知后十个工作日内未整改， 则采购人有权自己进行或委托第三方进行必要的纠正， 一切风险与费用由供应商承担。

（9）除本协议另有规定外， 对中标供应商提交的质量保证与质量控制方案， 采购人的任何作为或不作为，均不会：

1）减轻或影响中标供应商遵守本协议或法律所要求的与质量保证有关的义务或责任；

2）被视为采购人应对质量保证与质量控制方案承担任何责任。

13 项目安全防护要求

（1）本项目服务实施期间，中标供应商应严格遵守国家相关安全规定。若因中标供应商责任出现任何安全问题，中标供应商应承担全部责任。

（2）中标供应商需证明其所提供的云服务满足公安部信息系统安全等保三级的要求（所需费用由中标供应商承担）。在合同有效期内，采购人可按需要求中标供应商提供证明材料。

14 项目管理要求

（1）采购人服务的项目最终客户包括地市相关单位，最终客户有参与和自身相关服务管理、评价的权利。中标供应商应及时响应采购人和最终客户的服务要求。

（2）采购人有权随时自己或委托监理单位检查中标供应商的服务是否符合本项目的要求。

1）若发现任何部分不符合要求， 采购人有权通知中标供应商，指出不符合规定之处。

2）若中标供应商对采购人根据上述第（1）款所发出的通知有异议，则须于接到采购人通知后的七日内将其异议及理由书面告知采购人，否则应提出整改方案和措施报采购人批准后对服务进行整改。采购人与中标供应商须尽合理努力以求解决此项事宜。若该问题在中标供应商收到采购人通知后十四日内不能得到解决，则依据争议解决程序就该事直进行解决。

（3）采购人是否监督、检验本项目均不能减免中标供应商在本项目业务要求下的任何义务、责任。

附：

《保密协议》

甲　　方：

注 册 地 址：

法定代表人\授权代表：

乙　　方：

注 册 地 址：

法定代表人\授权代表：

鉴于：

甲方是东莞市政务云平台资源服务的采购方，乙方为甲方提供东莞市政务云平台资源服务（以下简称“项目”）。

乙方按甲方对东莞市政务云平台（以下简称“云平台”）的规划和要求，承担政务云平台的基础设施即服务、平

台即服务、容灾备份服务、安全服务、机房服务以及迁移服务等服务的建设、提供及运行维护工作。

甲乙双方就该项目合作过程中，乙方为甲方提供云平台资源租赁服务，甲方在工作过程中向乙方提供有关保密信息，且该保密信息属甲方合法所有，乙方（包括但不限于乙方员工、代理人、顾问等）承诺负保密义务；

乙方确保在此项目中获取的甲方和用户方相关信息（包括但不限于数据、源代码、技术文档、商业秘密、任何技术性资料、以及甲方为完成东莞市政务云平台资源服务合同<以下简称“云平台合同”>及本协议提供的任何其他信息资料并且在提供时未说明是公开信息的），未经甲方书面许可，乙方（包括但不限于乙方员工、代理人、顾问等）不得将从甲方及用户方获取的一切资料和信息拿到云平台合同及本协议范围之外使用，否则全部收益归甲方所有，甲方有权暂停乙方的成交资格，并保留追究乙方责任的权利。

本协议保密信息是指：

在合作过程中，乙方（包括但不限于乙方员工、代理人、顾问等）接触到的相关内容，与合作有关或因合作产生的任何商业、技术、运营数据或其他性质的资料，包括但不限于数据、源代码、技术文档、商业秘密、任何技术性资料、以及甲方为完成云平台合同及本协议提供的任何其他信息资料并且在提供时未说明是公开信息的。

无论以何种形式或载于何种载体，无论在披露时是否以口头、图像或以书面等方式表明其具有保密性。

上述保密信息可以以数据、文字及记载上述内容的资料、光盘、资料、图书等有形媒介体现，也可通过口头等视听形式传递。

权利与义务：

乙方（包括但不限于乙方员工、代理人、顾问等）不得将获取到的相关内容（包括但不限于数据、源代码、技术文档、商业秘密、任何技术性资料、以及甲方为完成云平台合同及本协议提供的任何其他信息资料并且在提供时未说明是公开信息的、单位及个人隐私信息等）泄露给他人，不得翻阅与工作无关的文件和资料，不得从事其他与协议无关的工作。

乙方（包括但不限于乙方员工、代理人、顾问等）不得擅自记录、复制、拍摄、摘抄、收藏在工作中涉及的秘密和敏感信息，包括系统数据、第三方代码、接口等，不得将工作中涉及的相关项目技术方案及实施规划透露给他人。

乙方及乙方工作人员不得将在工作中获得的相关信息透露给他人，严禁私自下载、拷贝计算机内数据信息，不得擅自携带记载工作内容的硬盘、U 盘和打印资料外出，严禁将系统的程序、口令、密钥等泄露给特任。

乙方对其参与本项目的员工定期组织保密制度培训，并与其工作人员签订与本协议要求内容相同的保密协议，保密协议有效期同本协议且不因员工从乙方离职而中断。乙方应确保有关人员遵守本协议并提交参与本项目员工的有关资料（如：身份证复印件、职称证明、项目经验等）给甲方，如需更换员工需事先征得甲方同意并提交相应的资料。

上述限制条款不适用于以下情况：

在签署本协议之时或之前，保密信息已以合法方式属接受方所有；

保密信息在通知给接受方时，已经公开或能从公开领域获得；

接受方应法院或其他法律、行政管理部门要求的披露信息（通过口头提问、询问、要求资料或文件、传唤、民事或刑事调查或其他程序）因而透露保密信息，在该种情况发生时，接受方应立即向披露方发出通知，并作出必要说明。

双方均不保证保密信息的精确性与合理性。

保密信息披露方提供的保密信息，如涉及侵犯第三方知识产权的情况，接受方不对此侵权行为负责，且免于由此产生的索赔。

违约责任：

乙方对在履行云平台合同及本协议过程中所接触的工作秘密（包括但不限于数据、源代码、技术文档、商业秘密、任何技术性资料、以及甲方为完成云平台合同及本协议提供的任何其他信息资料并且在提供时未说明是公开信息的、

单位及个人隐私信息以及甲方为完成云平台合同及本协议提供的任何其他信息资料并且在提供时未说明是公开信息的）承担保密义务。未经甲方书面许可，乙方（包括但不限于乙方员工、代理人、顾问等）不得将从甲方及用户方获取的一切资料和信息拿到云平台合同及本协议范围之外使用，否则全部收益归甲方所有，并另行赔偿甲方及用户方因此遭受的全部损失，并保留追究乙方责任的权利。

免责条款：

由于地震、水灾、火灾或政策变化等人力不能预见、不能避免、不能抗拒的原因，导致甲乙双方或一方不能履行或不能完全履行本协议项下的有关义务时，甲乙双方相互不承担违约责任；在不可抗力影响消除后的时间内，一方或双方应当继续履行本协议。

本协议有效期自主合同《东莞市政务云平台资源服务合同》（合同编号：　　）签订之日起，至服务期限届满后三年截至，无论本合同是否切实得到履行或因任何原因变更、解除、终止、失效等，本条款均始终有效。

争议解决：

本协议受中华人民共和国（以下简称“中国”）的法律管辖并按照中国的法律进行解释，如双方无法协商解决，应提交甲方所在地人民法院诉讼解决。

经双方书面确认，任何一方不得变更或修改本协议，国家另有规定的除外。

本协议未尽事宜，双方可签订补充协议。补充协议为本协议不可分割的一部分，与本协议具有同等效力。

本合同一式五份，其中甲方壹份、乙方贰份、东莞市公共资源交易中心、政府采购管理机构各执壹份。

本协议自双方签字盖章之日起生效。

甲方（盖章）：	乙方（盖章）：
地址：	地址：
授权代表（签字）：	授权代表（签字）：
日期：	日期：