附件《采购需求》：

1、项目总体要求

1.1 项目目标

遵循“整体协同、集约高效、按需服务、共享开放、绿色安全”的原则，按照“共性优先、按需服务、急用先行、技术可靠”的要求，参照市政务云服务目录、服务单价和服务标准，向云服务商（投标人）租用区级政务云资源，以满足普陀区城市数字化转型需要，不断提升政府为民服务和社会治理水平。

1.2 项目要求

（1）投标人提供的政务云平台整体可用性应不低于 99.99%，数据可靠性应不低于 99.999%，对每一项云服务的可用性、可靠性等 SLA 指标进行明确描述；

（2）投标人应构建有效的高可用政务云平台，除分别独立为用户提供私有政务云服务外，还需形成数据共享机制，可在最短时间内对用户的应用系统进行快速响应、处置和恢复；

（3）投标人应严格执行国家、地方、行业各项有关本项目业务管理和安全作业的法律、法规和制度，积极主动加强和服务业务及安全等有关的管理工作，并按规定承担相应的费用。投标人因违反规定等原因造成的一切损失和责任由投标人承担；

（4）构建于政务云平台上的各部门业务系统、所有数据的拥有权及使用权均属于政府，投标人无权对其进行支配，所有设备的维修、报废等处理需经政务云主管部门同意，并在监管下进行。若发现投标人未经许可对业务系统和数据进行支配，招标人将对投标人采取惩罚措施并追究其法律责任；

（5）投标人确认的用于项目的设备规格型号和数量，必须与投标文件承诺一致，未经招标人书面批准不得随意调换或更改，若自行调换或更改，按照合同违约处理；

（6）投标人在中标后履行政务云服务的过程中，需遵守《上海市政务云管理暂行办法》《上海市大数据中心市政务云服务商服务考核标准（试行）》《普陀区政务云管理暂行办法》的管理要求，若违反文件相关规定，按照合同违约处理；

（7）在政务云服务目录、服务单价不变的情况下，投标人在服务期内每年通过签署补充协议或备忘录对当年度的政务云服务绩效目标、SLA 服务要求、用户满意度目标以及服务目录细则予以确认和约定；

（8）投标人确认的项目运维团队人员及数量，必须与投标文件承诺一致，未经招标人书面批准不得随意调换或撤离，若自行更换或撤离，按照合同违约处理；

（9）投标人承担政务云平台（主要包括物理资源、计算资源、存储资源、网络资源）以及数据防篡改、防丢失的安全责任；

（10）投标人需根据招标人要求提供云用户应用上云所需的测试资源，免费提供服务；

（11）软件合法、合规授权，满足知识产权方面的有关规定和要求。

2、项目范围及要求

2.1 招标范围

投标人应提供以下各项云服务（下述服务内容不得缺失）：

（1）基础设施服务：为政务云用户提供机房资源服务、物理托管服务、网络资源服务、计算资源服务、存储资源服务；

（2）软件支撑服务：为政务云用户提供支撑服务、安装服务、维护服务、应用入云部署服务；

（3）信息安全技术服务：为政务云用户提供安全防护服务、用户安全服务、安全接入服务、安全管理服务、安全扫描服务、网站防护服务等，应配合招标人完成各项安全检查工作。

（5）应用迁移服务：包括应用入云迁移前期调研、配合设计及实施服务，迁移过程中应具备相应数据备份保障能力。

（6）云管服务：投标人应基于云管平台，提供自动计量计费服务，支持每月按 23 项服务目录对政务云整体、云使用单位虚机、信息系统进行分类和汇总查询统计，同时可以通过相关计费工单下载查阅证明材料；提供云资源监控和预警服务，对政务云整体、云使用单位虚机、信息系统的 CPU、内存、存储等使用率指标进行监控，并对云使用单位虚机、信息系统形成告警记录，以实现云资源使用能效的优化提升；定期对信息系统开展资源评估，并提供云资源调优服务。以上监控、查询、统计等数据应能够以云管平台接口形式对接给招标人。招标人及投标人在合同签订 30 日内完成需求确认，超出部分协商确认。

针对以上各项云服务内容，投标人应建立并提供相应的运行保障服务制度、机制和平台：

（1）制度保障：投标人应提供保障政务云安全可靠运行的相关制度和规范，包括但不限于运行维护制度、安全保障制度、应急预案等。

（2）机制保障：投标人应建立政务云平台运行保障服务机制，包括但不限于政务云平台的资源监测、资源配置、资源优化、服务监控、事件处理、运维流程、日常巡检、重保服务、备份恢复、应急演练、服务质量监督和周期运营报告等。

（3）平台保障：投标人应通过云管平台向招标人提供所需的服务工单、计量计费、统计查询、监测预警、接口对接等功能和服务，并作为本项目开展服务费结算的基础。

2.2 服务目录

投标人应根据拟投标包件，对应以下服务目录及单价，制作报价单进行报价。以下服务目录计量单价为元/年。

第 1 包：

序号	服务类别	服务子类	服务项	服务子项	单位	单价（元/年）
1	基础设施服务	机房资源服务	机房空间服务	机房空间服务	平米	15600
2		物理托管	机房机柜服务	整机柜租用	个	42000
3		网络资源服务	互联网公有 IP 服务	互联网公有 IP 服务	个	113
4			互联网带宽（骨干级）	互联网带宽（骨干级）	GB	450000
5			应用负载均衡服务	应用负载均衡服务	每 IP	240
6			安全交换区	安全交换区（网闸）	每 IP	9600
7		计算资源服务	CPU	CPU	核	180
8			内存	内存	G	180
9		存储资源服务	应用存储空间	应用存储空间	TB	960
10			高性能数据库存储	数据库存储	TB	1800
11			数据备份服务	数据备份服务	TB	960
12			数据归档服务	数据归档服务	套	2100
13	软件支撑服务	应用入云部署服务	应用部署	调研、制定方案、测试、部署、应用迁移、测试迁移等	次	5000
14	信息安全技术服务	安全防护服务	网络访问控制服务	网络访问控制服务	租户	20000
15			入侵防御服务	入侵防御服务	租户	1800
16		用户安全服务	用户管理服务	用户管理服务	租户	6600
17			用户身份认证服务	用户身份认证服务	租户	6600
18		安全接入服务	VPN 接入	VPN 接入	隧道数	7200
19		安全管理服务	数据库审计服务	数据库审计服务	实例	5400
20		安全扫描服务	常规安全漏洞扫描	常规安全漏洞扫描	次	690
21			系统上线安全扫描	系统上线安全扫描	VM/次	690
22		网站防护服务	在线防护 WAF	在线防护 WAF	套	4140
23			网页防篡服务	网页防篡服务	套	7000

第 2 包：

序号	服务类别	服务子类	服务项	服务子项	单位	单价（元/年）

1	基础设施服务	机房资源服务	机房空间服务	机房空间服务	平米	15600
2		物理托管	机房机柜服务	整机柜租用	个	42000
3		网络资源服务	互联网公有 IP 服务	互联网公有 IP 服务	个	113
4			互联网带宽（骨干级）	互联网带宽（骨干级）	GB	450000
5			应用负载均衡服务	应用负载均衡服务	每 IP	240
6			安全交换区	安全交换区（网闸）	每 IP	9600
7		计算资源服务	CPU	CPU	核	180
8			内存	内存	G	180
9		存储资源服务	应用存储空间	应用存储空间	TB	960
10			高性能数据库存储	数据库存储	TB	1800
11			数据备份服务	数据备份服务	TB	960
12			数据归档服务	数据归档服务	套	2100
13	软件支撑服务	应用入云部署服务	应用部署	调研、制定方案、测试、部署、应用迁移、测试迁移等	次	5000
14	信息安全技术服务	安全防护服务	网络访问控制服务	网络访问控制服务	租户	20000
15			入侵防御服务	入侵防御服务	租户	1800
16		用户安全服务	用户管理服务	用户管理服务	租户	6600
17			用户身份认证服务	用户身份认证服务	租户	6600
18		安全接入服务	VPN 接入	VPN 接入	隧道数	7200
19		安全管理服务	数据库审计服务	数据库审计服务	实例	5400
20		安全扫描服务	常规安全漏洞扫描	常规安全漏洞扫描	次	690
21			系统上线安全扫描	系统上线安全扫描	VM/次	690
22		网站防护服务	在线防护 WAF	在线防护 WAF	套	4140
23			网页防篡服务	网页防篡服务	套	7000

2.3 报价要求

本项目按照“先用后付、按实结算”的原则，参照市政务云服务目录、服务单价和服务标准，结合原政务云项目建设实际情况以及云服务需求实际，进行本项目报价：

（1）同预算金额,超过各包件最高限价的投标不予接受，且提供的每项服务类别单价不得超出上述服务目录中综合单价限价。

（2）投标人应根据项目采购需求，对云资源及云服务进行需求分析，对应上述服务目录和单价，测算服务量和服务费，并制订云服务方案，进行项目报价。

（3）上述服务目录和单价均为综合单价，投标人所报单价应包含认为完成该项目建设及服务所需的所有费用（如人工、材料、设备、管理费用、利润、税金等），以作为按实结算的依据，并承担一切价格风险。

（4）针对上述服务目录和单价中的每项服务，投标人的报价单均应进行填报服务数量及服务单价。投标人如有报价为 0 元或其他明显低于成本价（人、机、料成本）及违反内在价值规律的不正常报价行为，请在投标文件中提交相应的成本依据证明材料。

（5）投标人应在开标一览表中填报本项目服务期费用的总价。在项目服务期内，按实结算，投标报价不得超过各包件最高限价。请投标人根据自身及项目情况合理考虑相关报价风险后进行投标。

说明：第 1 包与第 2 包主要区别在于资源体量不同，而对于采购内容、技术指标、服务能力要求保持一致。本次项目的两个包不支持同一家投标人中标，若投标人同时投标两个包，第 1 包和第 2 包的技术投标内容和报价需保持一致。

2.4 云服务商（投标人）职责要求

投标人主要职责包括：

（1）负责政务云的建设、运维和安全保障，提供故障处理、应急抢修、系统升级、咨询培训等运维服务，保障政务云安全、平稳、高效运行；

（2）提供 5*8 小时驻场服务，以及 7*24 小时专用电话不间断技术服务，服务响应时间不超过 5 分钟。发生重大事件或紧急情况时，应及时提供调查报告并附佐证材料；

（3）保障政务云在重大节假日以及其他重要会议、活动期间的正常平稳运行；

（4）每月向招标人提供政务云运行报告，报告内容包括但不限于：云资源申请发放情况、信息系统使用情况、政务云运行情况、政务云安全分析、优化建议意见等；

（5）提供并执行区政务云应急预案，定期组织开展应急演练工作（每年不少于一次）；

（6）确保每年通过信息安全技术网络安全等级保护三级测评；

（7）其他需要投标人提供的支撑服务。

2.5 资源管理要求

投标人应当配合招标人建立普陀区政务云资源统筹管理制度，遵循“整体协同、集约高效、按需服务、共享开放、绿色安全”的原则，按照“共性优先、按需服务、急用先行、技术可靠”的要求，配合招标人分配和调节政务云资源，具体包括但不限于以下工作：

（1）资源开通：云使用单位提交资源申请需求，招标人审核通过后，投标人应当在五个工作日内完成政务云资源开通。

（2）资源扩容：云使用单位提交扩容申请，经招标人审核通过后，投标人应当在五个工作日内完成政务云资源扩容。

（3）资源回收：不再使用的政务云资源，由云使用单位向招标人提交回收申请，经招

标人审核通过后，投标人应当在五个工作日内完成政务云资源回收。

（4）测试资源：投标人需根据招标人要求提供云用户应用上云所需的测试资源，免费提供服务。

（5）优化使用：投标人应配合招标人加强对政务云资源使用的监测，有下列情形之一的，报招标人审核后予以警告提示，责令整改：

1）使用率长期较低；

2）僵尸系统长期占用政务云资源；

3）其他使用不规范的情形。

2.6 迁移支撑要求

投标人应在项目服务期内配合云使用单位做好应用上云及整体迁移工作，确保平稳过渡、顺利迁移。投标人应配合云使用单位对上云及迁移业务系统进行调查摸底、制定上云及迁移方案，迁移方案需要科学、合理、可实施。投标人应制定政务云平台使用规范、政务云安全防护管理办法等规范标准，协助云使用单位进行相关业务应用系统的部署、运行和安全保障。

应用系统迁移上云工作应当在保障原系统正常使用的前提下实现相应策略。对于 7*24 小时重要业务可实现在线迁移，保证业务连续性。需要根据云使用单位需求制定对应的迁移工作流程，要求迁移过程和迁移时间可控，按用户规定最小时间点实现业务顺时迁移。

2.7 云管服务要求

投标人应为本项目组建专业的技术服务团队，提供 7×24 小时的技术服务；技术服务团队的人员构成应涵盖本项目涉及的各个技术领域，具备云平台服务相关的经验和专业技能。

每个投标人应分别为普陀区政务云单独建立管理组织，配置相应团队。标包一提供至少 1 人的驻场运维服务，标包二提供至少 1 人的驻场运维服务。

驻场人员变更必须征得招标人同意，新驻场人员需通过招标人面试。对招标人提出的服务请求，投标人应在 5 分钟内响应，并安排相应的技术人员提供服务。投标人应提供运维团队成员名单及职责，并建立包含招标人在内的有效沟通机制。

投标人主要负责政务云机房运维、云基础设施运维、网络运维、安全运维、提供的应用服务运维以及日常基础功能运维（工单、日志）等。具体包括但不限于以下工作：

（1）负责对政务云相关软硬件、网络、平台的现场巡查、监控、维护，开展故障处理、应急抢修、系统升级、咨询培训等运维服务，保障政务云安全、平稳、高效运行。

（2）监控云资源使用情况，及时解决云使用故障，提供 5*8 小时驻场服务，以及 7*24 小时专用电话不间断技术服务，服务响应时间不超过 5 分钟。

（3）保障政务云在重大节假日以及其他重要会议、活动期间的正常平稳运行。

（4）对政务云运行状况进行统计分析评估，提出调整优化建议。

（5）政务云实行 24 小时不间断运行，应保持连续电力供应，如市电供应中断，应提供至少两小时电源保障。

（6）投标人按要求指派政务云现场驻场运维服务人员，驻场运维人员应依据招标人考勤管理制度进行考勤登记。

2.8 安全保障要求

投标人主要负责政务云机房、云基础设施及云管平台等的安全保障，具体包括但不限于以下工作：

（1）按照国家信息安全相关规定，建立健全安全保护工作制度，加强安全监测和防御工作，监控网络行为，阻断网络攻击，做好数据备份，开展应急演练，定期开展网络安全等级保护测评（测评得分不得低于 85 分），保障政务云安全稳定运行。

（2）当云使用单位出现严重影响政务云整体安全稳定运行且响应不及时的情况，投标人可以在告知云使用单位后，暂时中断该单位云服务，待事件处理完毕后恢复服务。

（3）未经云使用单位授权，任何单位和个人不得进入云主机、云数据库、云存储等用户资源，不得泄露、篡改、毁损、复制和利用用户数据；不得利用政务云侵犯国家、集体利益以及公民的合法权益，不得利用政务云从事违法犯罪活动；非法获取国家秘密构成犯罪的，依法追究其刑事责任。

（4）投标人应建立网络安全人员管理工作机制，明确网络安全责任人，落实关键岗位、职责和人员。

（5）投标人应提供完备的基于云的容灾备份体系，保障用户业务连续性和数据安全性，应具备为用户业务系统提供的备份恢复能力。

（6）政务云平台需符合网络安全等级保护基本要求第三级安全通用要求和云计算安全扩展要求，符合《信息安全技术云计算服务安全能力要求》（GB/T 31168 增强型）要求。

2.9 应急响应要求

投标人应根据故障情况，及时对故障进行上报及解决。故障解决的起始时间以监控告警时间或云使用单位报障时间中靠前的时间为准，结束时间以受故障影响的所有系统恢复的时间为准。

投标人应制定详细的《应急演练方案》，内容包括但不限于政务云平台的网络、存储、备份等，并按方案进行应急演练，服务期内应不少于 1 次。

招标人有权要求投标人提供全量与故障相关的过程信息，包括但不限于技术资料、实施资料和日志信息等，投标人应在发生故障 3 个自然日内准备好相关信息备查。投标人在处理完故障后，应按期将故障相关情况书面报告招标人，故障报告至少应包括以下内容：

（1）故障的类别；

（2）故障影响范围；

（3）故障的级别；

（4）故障发现时间；

（5）故障通报时间；

（6）故障解决时间；

（7）受影响的系统及影响内容；

（8）影响残留（未能解决的问题或隐患）；

（9）其他要求的内容。

3.项目服务内容

3.1 基础设施服务

基础设施资源服务：包括机房资源服务、网络资源服务、计算存储资源服务、云计算虚拟化服务。

1．系统架构：满足普陀区区级政务云总体架构要求，以政府购买服务的方式，依托政务外网，统一为云使用单位提供服务。

2．区级政务云平台结构：政务云平台的网络区域按政务网络安全要求划分为政务外网和互联网两个区域，政务云平台相应划分为两个部分，分别位于电子政务外网区域的政务外网云平台和位于互联网区域的互联网云平台。

3．硬件资源池：基于本区范围内的全面调研，两个标包总体资源指标不低于：CPU 2000 核、内存 8000 GB、存储 400 TB。其中标包一的资源指标不低于 CPU 1100 核、内存 4400GB、存储 220TB；其中标包二的资源指标不低于 CPU 900 核，内存 3600G，生产存储 180TB。

4．云运营运维平台：投标人应使用自主的、开放的、适应国际标准的商业化虚拟化软件，并搭建统一的个性化云运营运维平台提供服务。云运营运维平台能够基于 OpenStack 架构的虚拟化软件，提供云运营管理服务和云运维管理服务，能够对 IT 基础设施进行统一

管理。云运营运维平台支持主流虚拟化软件。

5．容灾备份：投标人应提供完备的基于云的容灾备份体系，保障用户业务连续性和数据安全性，具备对政务云平台本身的灾难恢复能力以及为用户业务系统提供的备份恢复能力。

6．安全服务：政务云平台需符合网络安全等级保护基本要求第三级安全通用要求和云计算安全扩展要求，符合《信息安全技术云计算服务安全能力要求》（GB/T 31168 增强型）要求。

3.1.1 机房资源服务

提供投标人自有机房，用于政务云平台部署及用户资产托管，机房相关设计指标如下：

编号	项目	设计指标
1	环境要求	温度：开机时 23℃ ±1℃，停机时 5℃ ～35℃；相对湿度：开机时 40% ～55%，停机时 40% ～70%；温度变化率＜ 5℃/h，不得结露。
2	结构	抗震：乙级以上，抗震烈度 7 度及以上，机房活荷载标准值≥8kN/m2，电池室≥16kN/m2，机房外墙不宜设采光窗，耐火等级：一级。
3	空气调节	机房专用空调 N+1 冗余，制冷量按 300W/m2 估算，总冷量负偏差不大于 5%；空调系统供电应采取双路市电自动切换线路供电，每台空调应采用独立回路供电。
4	供电电源	主机房由 2 个供电局向、2 个不同路由同时供电，保证电源不同时受到损坏，配备电源自动切换系统，切换时间小于 4 毫秒，供电系统可用性（由市电至机柜计算）≥99.99% ，单相负荷应均匀地分配在三相线路上，并应使三相负荷不平衡度小于 20%。
5	后备用电	需采用单路 240V 直流+单路市电直供，240V 直流系统电池满负荷放电时间约 30 分钟。 配备柴油发电机组，保障机架满负荷情况下可靠供电运行 6 小时。
6	电源质量	240V 系统输入电压额定值为三相 380V、允许变动范围 323V～418V；输入电压总谐波含量≤5%；输入频率 50Hz、变动范围±2.5Hz；稳压精度优于±0.6%。
7	接地	接地电阻≤ 1Ω，接地电位差<1V。
8	静电电位	主机房内绝缘体的静电电位不应大于 1kV。
9	机房布线	采用光缆或六类及以上对绞电缆，采用 1+1 冗余。

编号	项目	设计指标
10	照明要求	眩光限制按 I 级标准，照度按机房≥300Lux 及按现场布局排列，机房内应设置备用照明，其照度为一般照明的 15%。机房应设置疏散照明和安全出口标志灯，其照度不应低于 0.5LUX。
11	机房监控	空气质量：对温度、相对湿度、压差、含尘度；漏水监测报警；监控 IT 设备、空调、新风、动力、供配电系统、不间断电源、电池、柴油发电等设备。
12	安全防范	在主要出入口、机房、配套区域采用门禁系统和视频监控系统，机柜区域配备专用门禁和 24 小时监控系统，云服务商（投标人）应客户要求提供视频监控画面，监控录像保存时间不小于 3 个月。
13	消防	应配置气体消防系统和火灾自动报警系统。
14	其他	提供 10 平方米以上的相对独立的办公区域，并提供办公座位和桌椅，提供到机房的物理独立的网络连接。

3.1.2 网络资源服务

3.1.2.1 机房传输链路与网络环境

1.网络搭建和部署服务满足“云网合一”建设原则，政务外网接入由招标人提供，互联网及带宽由投标人提供，并按照互联网统一出口的安全管理要求进行集中管理。

2.政务云平台本身所使用的网络按照功能划分为政务外网和互联网，为了保护不同网络之间数据的传输安全，需要按照等级保护标准将这两个网络进行逻辑隔离。

3.政务外网接入：承载政务云平台的网络和区政务外网骨干传输网络高效安全地衔接，满足云使用单位接入政务云业务系统的网络需要。

4.互联网接入：承载政务云平台的网络和区政务外网互联网统一出口高效安全地衔接，满足云使用单位业务系统接入互联网的需要。每个云服务商（投标人）提供至少 1 路互联网出口带宽不低于 500Mbps，满足弹性 IP 配置的需求，预留 128 个公网 IP 地址。

5.投标人提供必要的配合，并按相关规范要求做好网络对接和安全防护。

6.专线要求：每个政务云平台采用冗余专线链路与区政务外网连接，接入点为区政府指定机房，提供 3 个 10Gb 链路，并实现双路由互为冗余。

3.1.2.2 政务云网络能力

普陀区政务云网络需要与现有机房对接，采用统一的政务外网出口。针对现网情况，网络服务能力体现在如下几个方面：

1.平台网络接入到普陀政务城域网，满足与原有平台的互联互通，具备快速收敛、高转发性能、易维护、易管理和节能环保等特性。

2.平台网络具备高可靠性、高可用性。网络设计能有效地避免单点故障，在设备的选择和关键设备的互联时，应提供充分的关键设备冗余、重要业务模块冗余和链路冗余，网络应当达到电信级可靠性。

3.平台网络架构具备高扩展性，不仅满足当前需要，也能满足未来业务扩展需求。

4.平台网络具备安全隔离能力，实现政府各部门之间网络层面的隔离。

3.1.3 计算存储资源服务

普陀区政务云平台需要满足现网过保设备承载业务的迁移。考虑到业务系统性能需求不同、数据存储类型不同（结构化、非结构化、半结构化），因此普陀政务云平台计算资源需求如下：

1.云平台需要支持根据业务应用的不同特点分配不同的计算资源，包括采用合理的物理服务器。

2.能根据业务应用的特点对服务器或存储进行配置，满足应用对计算和存储的需要（CPU、内存、网络 I/O、存储 I/O）。

3.满足不同数据类型的存储需求，提供 SAN、NAS 资源池。

4.计算平台需要和管理平台联动，实现对虚拟计算资源的部署和分配。

3.1.4 云计算虚拟化服务

1．根据服务器功能分类和业务应用的性能需求，经评估业务应用可虚拟化，提供选择相应虚拟机规格类型。

2．根据各系统对 CPU、内存、网络和存储 I/O 的不同需求，对虚拟机规格进行分类，根据不同的操作系统，选择对应的虚拟机镜像，将虚拟机分布在相应的 x86 物理机上。

3．虚拟化平台管理提供以下服务：

1）基础云资源管理服务：对各类硬件资源、虚拟化资源进行统一配置、监控和管理。

2）云平台监控管理服务：提供关键性能指标的监控服务，如 CPU 利用率、内存利用率等，并提供图形展示界面。

3）虚拟网络管理服务：提供逻辑隔离区域，可提供定制网络拓扑、部署云计算资源，实现安全、可靠的私有云环境的搭建。

3.2 信息安全技术服务

1.信息安全技术服务：包括安全防护服务、用户安全服务、安全接入服务、安全管理

服务、安全扫描服务、网站防护服务、租户侧安全资源池等。建立健全满足云安全监管需要的配套检测、监管手段及相应监测办法。

2.投标人提供的政务云平台应满足《信息安全技术云计算服务安全能力要求》（GBT 31168-2014）、《信息安全技术云计算服务安全指南》（GBT 31167-2014）、《关于加强党政部门云计算服务网络安全管理的意见》（中网办发文[2014]14 号）及国家主管部门发布的其他标准规范要求。以平台通过等保三级 2.0 测评，安全体系符合国家等保三级测评要求且测评得分不得低于 85 分，由投标人负责组织测评负担测评费用。投标人需对平台级安全负责，并为其上运行的租户（及应用）可提供租户级安全服务能力，应用级安全由用户负责。

3.由于普陀区政务云平台的高安全性要求，通过构建互联网区、电子政务外网区及安全域来保证业务的安全性、便利性和可服务性。对云平台进行安全域划分，对不同安全域按照相应安全等级要求进行安全管理、用户与身份、数据安全、应用安全、IT 基础设施安全（包括网络安全与主机安全）、物理安全等安全防护。

4.提供云计算平台内虚拟化基础设施的安全保护能力，确保虚拟机的隔离，以及虚拟机自身系统的安全性。

5.满足国家安全等保三级要求，应具备防护服务能力，包括但不限于 WAF、IPS、防火墙、数据库审计、日志审计、主机防病毒等。

安全服务分类	安全防护能力	服务内容描述
物理安全	机房安全	投标人用于建设政务云服务中心的机房需满足国家 A 级（GB50174-2008）的安全要求。
网络安全	访问控制	政务云平台在各网络边界处均应部署安全访问控制设备，包括防火墙、IPS、VPN 网关、安全网关等，能根据会话状态信息为数据流提供明确的允许/拒绝访问的能力，控制粒度为端口级，同时系统具备对进出网络的信息内容进行过滤，实现对应用层协议的命令级控制，充分确保系统非实时在线层面的安全保护功能。
	安全审计	投标人按需对政务云平台使用网络设备运行状况、网络流量、用户行为等进行日志记录，能够根据记录数据进行分析并生成审计报表，同时对系统审计的记录进行有效安全保护，避免受到未预期的删除、修改或覆盖等不安全操作。
	边界完整性检查	投标人通过部署网络行为管理系统、安全审计系统应能够对非授权设备私自连到内部网络的行为及内部网络用户私自连到外部网络的行为

		进行检查，能根据用户信息、主机信息、IP 信息等准确定出非法互联位置，并对其进行有效的网络阻断控制。
	入侵防范	配备有 IDS 或 IPS 入侵防范、检测系统或安全网关系统，实现的实时防范功能应包括：端口扫描、强力攻击、木马后门攻击、缓冲区溢出攻击、IP 碎片攻击和网络蠕虫攻击等非法网络攻击行为，当检测到攻击行为时，系统将详细记录相关信息，同时在发生严重入侵事件时具备报警、记录功能。
	恶意代码防范	投标人在网络的边界处对各种恶意代码进行检测和清除功能，系统应支持自动及手工方式对恶意代码库的升级和检测系统的更新功能。
	网络设备防护	投标人所使用的网络设备均应支持对登录用户的身份鉴别功能，支持采用加密用户口令鉴、RADIUS 身份认证等方式，可通过命令行、Web、中文图形化配置软件等方式进行配置和管理，并可通过 ACL 访问控制列表的方式实现对网络设备的管理员登录地址进行限制，所有网络设备用户均应具备唯一标识。
主机安全	主机访问控制	主机系统应启用主机系统的访问控制功能，依据安全策略控制用户对资源的访问权限，通过系统的技术维护措施严格限制默认账户的访问权限，对重要信息资源设置敏感标记，并依据安全策略严格控制用户对有敏感标记重要信息资源的操作。
云管理平台安全	虚拟化安全	支持有代理或者无代理安全方式进行虚拟环境的整体防护；支持对虚拟机/模板进行安全扫描和防护，防止虚拟机/模板的安全策略/补丁更新不及时过期出现安全隐患；整体的虚拟化安全措施应避免“病毒风暴”。
	政务云平台安全	如果云管理平台需要数据库的支持，应保护好云管理平台的数据库安全，设置强壮复杂的密码策略、备份数据库和配置相关的网络安全服务；云管理平台的访问许可应加强管理，删除不需要的用户账号；安装云管理平台软件的操作系统需设置安全策略。
	应用安全整改配合	云使用单位部署在政务云平台中的应用系统在执行国家及本市有关电子政务信息安全管理办法的过程中，若发现重大安全事故或者安全隐患时，投标人需要配合进行安全整改。

3.3 应用迁移服务

应用迁移服务：包括应用入云迁移前期调研、配合设计及实施服务，迁移过程中能具备相应数据备份保障能力。

3.4.1 迁移服务内容

1.投标人在项目服务期内配合云使用单位做好应用上云及整体迁移工作，确保平稳过渡、顺利迁移。投标人上云支撑服务内容如下：

（1）对接上云方案

投标人及时响应对接云使用单位根据信息系统实际向招标人提出的书面上云申请。云使用单位所提供的上云方案中应包含计划上云信息系统的具体安全需求及设计，包括但不限于以下内容：信息系统功能说明（含网络拓扑图、系统架构图）、云资源需求、网络访问控制需求、备份需求以及部署时间安排等。

（2）上云方案审核

按照“合理规划、按需分配”的原则，对云使用单位所提交上云方案的完整性和合理性进行审核，云使用单位对审核后的上云方案进行确认。

（3）上云环境准备

投标人根据招标人工单以及确认后的上云方案，在二个工作日内为云使用单位开通云资源，并提供实施部署账号，云使用单位对云资源进行签收确认。

（4）系统上云部署

投标人配合云使用单位进行系统部署。

（5）系统安全检测

云使用单位完成信息系统上云部署后，投标人为上云系统提供必需的安全服务并通过第三方组织的系统上线前安全检测，可按照工单申请提供其他可选安全服务。

（6）系统上线发布

云使用单位通过系统安全检测后，报招标人审核通过后实施割接发布，投标人应做好相关配合保障工作。

（7）上云系统变更退出流程

云使用单位如有应用系统云资源变更或退出需求，应提交申请，经招标人确认后，由云使用单位、投标人按要求实施。对需要下线的信息系统，云使用单位应制定下线工作方案，并做好系统下线和数据迁移备份工作。投标人应提供下线系统镜像和数据保护，并在下线保护期结束后按约定完成镜像和数据删除工作，并将相关情况通报云使用单位。

3.4.2 迁移责任边界

1.安全责任边界

按照迁移标准提供迁移部署实施过程中的应用连续性、数据连续性相关的安全服务。

迁移前的安全体系与责任归属应用开发商和原单位负责。

迁移部署实施过程的数据安全保障由投标人负责，应用的安全由应用开发商负责。

迁移完成后的安全责任，基础设施与虚拟云环境的安全由投标人负责，应用的安全管理由应用开发商负责。

2.运维责任边界

相关虚拟环境、物理设备的运维服务由投标人负责。

对于迁移部署实施过程中迁移工具的运维服务，其中测试环境的运维与安全由投标人负责，应用系统本身的软件与数据的运维由原应用开发商负责。

3.5 云管服务

所有投标人完成自身云管理平台的搭建和部署，同时为招标人搭建一套统一的云管理和服务平台。

3.5.1 云运营运维平台

普陀政务云主要面向云使用单位提供相应的资源服务，云运营运维平台主要需求如下：

一、运营系统

平台实现统一的服务受理与交付管理系统，以便招标人或平台管理人员实现服务的申请、受理、发放和计量等能力。主要包括：

（1）提供服务门户，提供对各类服务的统一管理能力，以便招标人或平台管理人员可以通过目录服务功能实现对服务进行分类、定义、发布、更改、删除、查询等管理操作。

（2）对于通过门户提交的服务申请订单，平台管理人员可以通过订单管理功能进行处理。

（3）对于使用的平台资源的具体量，可实现计量及情况统计分析。

（4）能够为各云使用单位提供独立的账号，用于其管理自己申请的服务。

二、运维系统

普陀政务云平台具有平台系统复杂、提供服务众多、服务对象多样等特点。需要组建统一的基于云计算的运行保障支撑系统为平台提供运行保障服务以保障平台的服务质量达到用户的需求。运行保障服务需要面向基于云计算的平台运行维护者、公共平台的管理者以及平台的使用者（公众、公务人员以及机构用户）。

运维系统主要功能包括：

（1）实现对虚拟化环境、云计算平台和物理环境的集中监控和管理。管理的对象包括：数据库、操作系统、服务器、网络设备和安全设备、存储设备、机房设备。

（2）建立报表系统，实现对服务管理平台中各种信息的分析和呈现。

（3）具有良好的扩展性，以适应平台业务不断地发展；具有良好的开放性，以适应不同环境的管理要求。

（4）结合现状，运行保障服务需求。

（5）实现计算、存储及虚拟资源的统一监控、统一管理、统一维护。

3.5.2 云管理服务平台

面向招标人搭建一套云管理平台，提供资源监控、资源预警、自动计量计费、云资源调优等功能，该平台使用云投标人资源进行部署，并限定特定 IP 的 PC 终端访问。云管平台主要包括服务内容如下：

（1）情况总览

帮助招标人快速了解整个云平台的各项情况，包括各类资源信息、服务信息、监控信息等，并支持通过大屏进行展示。

（2）云管业务

实现各类云服务业务的管理，包括上云服务管理、云服务管理和退出服务管理，其中：上云业务包括现有业务应用系统的迁移上云服务和新建业务应用系统的部署上云服务。云服务指各云使用单位使用各类云服务（服务目录中包含的各类服务）的全过程跟踪管理。退出服务指业务应用系统从云上退出的流程管理。

（3）监控告警

资源监控和预警，对云使用单位业务虚机的 CPU、内存、存储使用率指标按月平均数进行监控，并对虚机形成告警记录，以实现资源能效的优化提升。

（4）资源管理

云资源调优，定期对信息系统开展资源评估，定期提供云资源的使用率情况。资源管理可分为云使用单位和云运行管理单位（招标人）两个层面。

1） 对云使用单位

实现对云使用单位在用资源的相关查询、查看以及相应的配置管理功能。同时，可进一步查看当前已上云业务应用系统的各类运行情况，并申请各类服务。

2） 对云运行管理单位

实现对云平台本身的各类资源管理功能，包括资源配备情况、运行情况、监控情况、故障记录等信息。

（5）计量计费

支持对普陀区大数据中心政务云整体、各云使用单位、项目应用三个层次按月对 23 项

服务目录的分类和计量计费汇总查询统计，包括基础设施服务（CPU、内存、存储等）、软件支撑服务、信息安全服务等，结合各投标人服务目录中的计价规则计算相应的费用，并提供相应的账单功能，同时可以通过计费相关工单下载查阅证明材料。计量计费结果作为云运行管理单位（招标人）向投标人进行服务费用按实支付结算的依据。

（6）统计报告

需提供基础报表功能，包括服务报告、事件报告、计量计费报告等。

（7）消息通知

搭建统一的消息通道，通过邮件、短信、站内消息等途径，发送平台各类消息，包括：服务审批/反馈消息、监控告警消息、故障事件消息等。同时发布各类通知、公告，并推送给各云服务商。

（8）系统管理

实现各类与具体业务无关的配置管理功能，包括：用户管理、角色/权限管理、组织机构管理、数据字典、流程配置等功能。

（9）接口服务

支持与其他系统的集成，支持向招标人提供开放接口，供招标人获取政务云相关数据。支持提供接口与市级政务云基础设施管理平台对接，实时归集区级政务云资源使用数据、平台运行数据等。招标人及投标人在合同签订 30 日内完成需求确认，超出部分需进行协商确认。

3.6 运维服务

3.6.1 运营保障管理服务

负责提供政务云平台的日常运营保障管理服务内容如下：

（1）提供热线电话、电子邮件和即时通信等技术支持方式，提供 7*24 小时电话响应服务，提供 5*8 小时的现场运营服务。

（2）日常运营与管理：对政务云平台进行资源管理、权限控制、组织机构维护、流程规范等服务。

（3）迁移及升级割接：开展业务系统迁移割接和政务云平台软硬件升级割接；投标人在升级前制定完善的操作实施方案并出具迁移及升级责任承诺书，在方案中尽量降低对上层业务系统的影响；对于可能影响上层业务系统的各类操作，应全面评估操作影响，并提前通知招标人具体操作计划安排，在招标人同意后方可执行操作。

（4）应急演练与应急响应：根据政务云平台高可用设计特性和各组件的重要性进行针

对性演练，制订应急预案，每年组织不少于 1 次应急演练。当发生重大应急事件时，招标人需在投标人的牵头下实施应急响应操作，并在事后制定重大事件报告。

（5）配置实施及管理：进行政务云平台各软硬件设备的基础配置、IP 配置、角色用途、账号密码等的统一配置实施及配置管理。

（6）政务云平台故障处理：处理政务云平台发生的各类软硬件、通信线路等故障，确保上层业务系统能够正常稳定运行；其中故障处理流程需要电子化并规定处理时限及当前处理环节的责任部门和责任人。

（7）系统中断：投标人在中标后由于维护原因，需中断系统进行平台升级操作时，提前至少 72 小时（重大自然灾害除外）通知招标人做好相关准备工作，征得招标人同意方可实施。

（8）安全加固：对政务云平台各个基础组件进行安全策略配置、安全扫描和系统漏洞的加固。

（9）故障处理和响应：投标人需对合同服务出现的故障响应做出相关保证。投标人应建立完善的私有云故障管理体系，管理体系涵盖故障处理的故障等级、职责分工和处理界面，每个处理流程留有电子化记录并在每个处理环节中落实到投标人的部门和相应的处理接口人。按照故障等级不同，需要有不同的处理时长和故障恢复时限。

（10）节假日保障：重大节假日期间进行政务云平台运行和信息安全的重点保障。

（11）运行保障服务：包括政务云平台的资源监测、资源配置、资源优化、服务监控、事件处理、运维流程、日常巡检、备份恢复、应急预案管理、服务质量监督和周期运营报告等服务。

（12）运营指挥服务：实现云平台的统一指挥、监控、管理、调度、应急处置等服务。

（13）建立健全配套的政务云安全制度与规范：投标人提供基于自身平台的相关标准、办法及建议，并组织安排专项的安全服务团队，如：提供政务云管理办法、运维制度、应急预案等。

（14）提供专职驻场服务及重要时期的应急值守服务，重大活动期间需确保业务骨干、管理人员到场并提前制订预案。

3.6.2 云平台运维服务

云平台所承载应用为区内核心应用，投标人应确保本项目服务范围内的应用系统在交付过程中对外持续服务，确保业务系统“0 中断”。且投标人所提供的服务方案中不应涉及需招标人额外协调的第三方支撑或成本支出。

服务项	服务内容
云平台运行管理	为政务云政务外网及互联网区域提供 7×24 小时的运行管理服务。
	云平台运行监控：通过云平台管理系统对整个云平台的资源使用情况、资源健康情况等进行 7×24 小时实时监控。
云资源规划管理	不定期收集各云使用单位提出的资源使用需求计划，对政务云所有资源进行规划管理；定期评估分析政务云资源使用情况，并按招标人要求提供相应的评估方案。
业务办理	资源开通：根据各云使用单位的新增资源需求，进行资源分配；搭建运行环境，包括但不限于配置虚拟机、存储、网络、操作系统以及相应的安全策略等，并配合各云使用单位完成业务系统的部署。
	新业务上线评估：对云平台范围内的新上线的业务系统进行安全评估，主要评估内容包括但不限于账号口令检查、服务与端口信息备案、防火墙策略检查、安全漏洞加固情况检查、安全配置合规率检查、日志功能记录检查等。
	在业务系统通过安全评估及信息安全评测后，开放相关业务端口，确保业务系统的正常上线运行。
	资源变更：根据各云使用单位的资源变更需求，对已部署的业务系统进行资源调整，包括但不限于计算资源、存储资源、网络资源、软件配置、安全保障等运行环境的变更调整。
故障处理	对云平台上运行的业务系统出现的故障，提供 7×24 小时的技术响应，配合招标人及时排除故障。
数据备份	按照各云使用单位提出的数据备份需求，定制数据备份策略。
	定期对备份数据进行恢复性测试，测试周期由招标人按需确定。
运维服务报告	根据云平台的整体运行，按需提供政务云平台服务报告。内容包括但不限于政务云平台运行情况、资源利用效率、业务开通办理、故障处理、用户技术支持以及数据分析等。
	针对各云使用单位出具单独的政务云平台服务报告，内容包括但不限于该单位业务系统在政务云平台的运行情况、资源利用效率、业务开通办理、故障处理、用户技术支持以及数据分析等。报告的周期由招标人按需提出要求。
日志审计	对云平台核心系统的日志审计分析，包括但不限于网络系统、虚拟化系统、存储系统、备份系统、云管理系统等；对其他各类日志进行审计。通过异常日志分析提前发现潜在风险并进行处理。

业务咨询	为各云使用单位提供云平台相关的业务咨询，包括但不限于资源申报、资源调整、业务系统迁移、与云平台网络对接、数据共享等。
技术支持	为招标人及云使用单位提供云平台使用过程的各类技术支持服务。
应急演练	制定云平台的运行维护应急预案，并组织定期演练，保障灾难发生时，能够保留数据、恢复系统及数据。

3.6.3 容灾备份服务

1.数据容灾服务：由投标人提供完善的备份方案，对政务云上的数据进行有效的数据备份；同时制定完善的灾难恢复机制，选取异地的机房设置灾备服务。

2.政务云平台本身的备份和恢复能力包括：

（1）政务云平台使用的防火墙、交换机、网络安全、服务器、存储等设备具备高可靠性及冗余性，即单个设备或单个节点出现故障时，其他设备/节点可以立刻接管任务，保证政务云平台整体的业务连续性不低于 99.99%。

（2）政务云平台具备高可用和动态迁移功能，发生物理设备故障后，虚拟机可以自动迁移到其他可用资源上运行，确保业务系统不受物理设备故障影响。

（3）政务云平台提供备份/快照功能，能对政务云平台中的物理和虚拟服务器进行备份，同时也能对虚拟化存储池进行存储镜像备份，防止存储损坏导致数据丢失。

3.政务云平台为云使用单位应用系统提供的备份/恢复能力包括：

（1）备份方式包括完整备份、差异备份和增量备份。

（2）备份工具支持 Windows 系列操作系统、Linux 主流系统操作系统、主流数据库软件、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；支持数据消重功能。

（3）备份服务器支持管理本地备份和同城异地备份。

（4）对备份过程状态、备份结果提供运维监控保障服务，确保备份任务执行成功以及备份的数据完整性。

（5）每年提供至少 2 次灾备演练服务。

（6）使用备份工具、备份服务器，将云使用单位的应用系统及数据在本地进行备份。

3.6.4 其他服务

普陀政务云上运行的业务系统数据所有权归各云应用系统所有人所有，未经数据所有人同意投标人不得通过任何手段收集、分析、处理、篡改政务云平台中的数据。禁止数据

以任何方式或渠道泄露出去，投标人须同招标人签订相关保密协议。

4、验收与考核

4.1 验收要求

服务期结束后，由招标人组织对投标人提供的服务是否符合招标文件的技术要求进行查验，之后由投标人按照招标文件的要求及与招标人共同商定的验收方案和验收标准，负责在规定时间内进行验收，并接受招标人的监督。

政务云验收服务需要提交的材料包含但不限于：服务方案、应急预案、应急演练报告、结算证明材料、项目总结报告、工单记录等。该部分对未来的验收实施、业务发放和业务维护至关重要，招标人和投标人双方都需要参与验收服务需求制定。

验收交付：在招标人和投标人确认验收服务结果后，投标人完成服务交付。

参考验收标准表如下：

按照政务云的服务模式，围绕技术要求和服务质量，提出如下的参考验收标准表格（仅供参考），包含验收的分类和验收子类。

投标人需按照自身的应标技术情况提供针对性的验收方案，包含但不限于以下验收项：

特性	评估项	评估内容
功能性	云平台功能接口	云平台提供的功能接口应符合市场主流接口技术标准。
	云资源管理功能	对云平台资源进行管理，资源监控预警、自动计费等。
资源效率	资源监控	应能够实时监控本次招标云平台中 CPU、内存、存储等资源的使用情况。
	管理接口	应提供一套管理接口，对本次招标云平台进行管理。
	应用支持能力	云平台应支持各类常用操作系统（Windows、Linux 等）的部署，支持各类常用中间件（Apache、Tomcat、IIS 等）、支持各类常用数据库（SQL、MySQL、Oracle 等）。
可靠性（业务连续性）	负载均衡	重要物理网络节点（防火墙、交换机、IPS）应考虑双机热备负载均衡设计。
	高可用性	应实现云平台中某一物理节点故障时，HA 虚拟机可在另一台可用的物理机上重启。
	动态迁移	应在服务不中断的条件下，实现虚拟机和存储的动态迁移。
	快照	应在服务不中断的条件下，实现虚拟机系统和数据文件的定期快照和增量快照。

	应急方案	应在统一的应急预案框架下制定不同事件的应急预案，包括应急组织机构、启动应急预案的条件、应急处理流程、系统恢复流程、事件信息收集、分析、报告制度、事后教育和培训等内容。
	应急演练	应定期组织单位和云运营者协同开展包括机房、网络、业务安全的应急演练。
	持续服务（自动重连）	与设备系统连接中断时，云平台应在 10 秒内自动尝试重建连接，再次失败应告警。
	网络冗余	客户与云计算平台之间的网络链路应采用多个优质链路，做到网络链接冗余。
信息安全性	网络隔离	应对云租户之间的网络进行有效隔离，自建云和运营商云间的网络隔离。
	资源隔离	应限制访问重要物理资源及虚拟资源、安全管理中心的远程登录地址，划分不同安全级别资源池，并实现资源池之间的网络隔离。
	访问控制	应对云中的租户进行唯一标识和鉴别，对特权账号实施多因子鉴别、抗重放鉴别机制。对云中的资源设置访问控制规则。
	身份鉴别强度	应建立策略机制，能够强制执行最小口令复杂度；对存储和传输的口令进行加密；强制执行最小和最大口令生存时间限制。
	访问路径	业务终端与业务服务器之间、管理终端与管理服务器之间进行路由控制建立安全的访问路径。
	攻击检测	应在物理或虚拟网络边界处部署入侵防范设备和恶意代码防范设备，检测网络攻击行为，并记录攻击类型、攻击时间、攻击流量等，对恶意代码进行检测和清除，并定期更新恶意代码库。
	远程执行权限	应对远程执行特权命令进行限制，并禁止非安全的网络协议。
	安全审计	云服务方应通过有效措施定制审计策略，收集相关审计数据。特别对特权租户行为和重要安全事件进行审计，并对审计记录进行分析和定期备份。
	信息安全性的依从性	云平台的信息安全性应符合国家信息安全等级保护三级要

		求。
维护性（运维）	电话支持	云平台提供方应提供热线电话、电子邮件和在线网站等技术支持方式，提供 24 小时电话响应服务，重要节点应强化保障。
	日常巡检	云平台提供方应制定维护管理规定和计划，周期性地对云平台进行日常监控、巡检，包括监控警告的处理，巡检异常的处理等。
	故障响应	应定期检查处理云平台发生的各类软硬件、通信线路等故障，确保上层业务系统能够正常稳定运行。
	故障处理	云平台提供方应建立完善的云平台故障管理体系，其涵盖故障处理的故障等级，职责分工和处理界面等，每个处理流程需留有电子化记录并在每个处理环节中落实到各部门和对应负责人。

4.2 考核要求

招标人对投标人提供的云服务开展考核，考核内容包括但不限于年度考核、云服务满意度考评，考核结果作为服务费结算的重要依据。在云服务提供过程中，如发生服务或安全相关问题，招标人将依据问题严重程度进行相应处罚。

考核满足以下条件：

（1）投标人需按照考核要求提供项目服务材料。若服务中涉及的服务内容存在不合理或不完整的情况，投标人有责任和义务在提出补充修改建议并征得招标人同意后付诸实施。

（2）投标人需针对政务云平台提供具备权威的信息系统安全等级测评机构出具的国家信息安全等级保护三级评测报告且测评得分不得低于 85 分，。

4.2.1 系统保密考核

投标人与招标人应签署保密承诺责任书。因投标人原因，导致发生数据外泄等系统保密事件，应承担由此给招标人造成的实际损失，并按相关规定追究责任。

4.2.2 安全知识产权

投标人提供的服务和交付的成果以及使用到的所有数据、文件、信息等引起任何第三方在专利权、著作权、商标权、名誉权、隐私权等权益方面向招标人或投标人的关联方及合作方（包括但不限于招标人的主管单位和招标人的合作单位等）发出侵权指控或提出索赔，或使招标人或招标人的关联方及合作方遭受任何处罚，应由投标人负责与第三方解决纠纷并赔偿全部损失，包括但不限于直接损失、间接损失、诉讼费 / 仲裁费、律师费、公

证费、鉴定费、保全担保/保险费等。

4.2.3 考核指标

投标人提供的政务云平台整体可用性、数据可靠性应不低于主流的政务云要求，即可靠性 99.99%。投标人应每月提供《服务质量月报》，内容包括政务云平台基本情况、云基础资源服务情况、信息安全服务情况、上云支撑服务情况、运维管理服务器情况、其他服务情况等。云服务商（投标人）应建立政务云年度考核指标体系，参照模板如下：

一级指标	分值	二级指标	分值	指标解释	应达要求	测量规则	评分标准
满意度管理（H）	30	云服务满意率（H1）	30	云服务满意率：见满意度调查问卷	每年满意度不低于 90%	云服务满意率：见满意度调查问卷	云服务满意度≥90%得满分，每偏差 1%扣除权重 2%，扣完为止
培训管理（I）	20	年有效培训次数（I1）	20	年有效培训次数：每年云服务商面向政务云使用单位的培训次数	每年有效培训次数不小于 6 次	每次培训人数不少于 4 人，按提供培训教材、培训通知、现场签到或会议记录等佐证材料计数	年有效培训次数≥6 次得满分，每偏差 1 次扣除权重的 5%，扣完为止
安全管理(J)	20	安全风险及时整改数（J1）	20	安全风险及时整改数：发现涉及安全风险事件时，在规定的时间内予以整改的数量	安全风险包括安全漏洞、故障隐患、第三方监管巡检发现的其他问题等应及时整改时间不超过规定时间	（1）安全风险整改时间=安全风险处理完成时间一发现安全风险的时间（2）安全风险及时整改数=按时整改数	云服务商的安全风险整改指标未达到要求，每发生一起则扣 2 分，扣完为止

	30	安全责任事故数（J2）	30	安全责任事故数：云服务商提供的机房、网络、安全、虚拟机、物理机、存储、运维等方面出现问题引起的安全责任事故数量	不发生该类事件	安全责任事故数=第三方监管出具监管报告确认为安全责任事故的数量	（1）云服务商的五级安全责任事故每发生一起则扣2分，扣完为止 （2）云服务商的四级安全责任事故每发生一起则扣4分，扣完为止 （3）云服务商的三级安全责任事故每发生一起则扣6分，扣完为止 （4）云服务商的二级安全责任事故每发生一起则扣8分，扣完为止 （5）云服务商的一级安全责任事故每发生一起则扣10分，扣完为止

故障定级可参照《上海市大数据中心市政务云服务商考核标准（试行）》，具体可由招标人及投标人在政务云合同中明确要求。

5、服务期：本期项目的整体服务期为一年，自实际提供服务之日起开始计算服务期。

6.支付方式：每年的服务费用支付分两次完成，进入服务期后，招标人按照每个投标人的投标价格的30%支付每年的首付款；每年的服务费用按照先用后付的原则，当年服务期完成后，按照服务结算结果支付年服务费的尾款。

6.2 费用结算

为避免项目整体费用超过预算，结算价不得超过合同价（**合同金额上限闭口包干**），若结算价超过投标价的部分由中标人自行承担。

服务期结束后，由招标人指定的监理方对本期项目的所有投标人的服务费用进行评估，结算根据本年度实际使用数量情况，按照对应的服务单价（服务目录）结算，扣除当年度考核和违约处罚金的相应额度，比对服务费限额标准后，最终得到本年度服务费的金额。

6.3 第三方监理

由与招标人签订委托协议的第三方监理单位开展费用结算相关监理工作。

提示：《开标一览表》报价以人民币元为单位取整数，其余各报价表中的价格均用人民币表示，单位为万元，精确到小数点后四位，请注意换算。

★说明：第1包与第2包主要区别在于资源体量不同，而对于采购内容、技术指标、服务能力要求保持一致。本次项目的两个包件不支持同一家投标人中标，若投标人同时投

标两个标包，第 1 包和第 2 包的技术投标内容和报价需保持一致。