



广州群生招标代理有限公司

项目名称：增城日报《增城之窗门户网站》系统等级保护测评建设
项目

项目编号：GZQS1901FC04038

竞争性磋商 文件

采购人：增城日报社

采购代理机构：广州群生招标代理有限公司

温馨提示：供应商投标/报价特别注意事项

一、投标/报价供应商请注意区分投标/报价保证金及中标/成交服务费收款帐号的区别，务必将保证金按采购文件的要求存入指定的保证金专用账户，中标/成交服务费存入中标/成交通知书中指定的服务费账户。切勿将款项转错账户，以免影响保证金退还的速度。

二、投标/报价截止时间前半小时将开始接收投标/报价文件，投标/报价截止时间一到，将不接收任何投标/报价文件，因此，请适当提前到达。

三、采购代理机构有可能在相近时间有多个项目进行开标，请投标/报价人授权代表到达开标会场后按指示前往相应的会议室，或主动咨询工作人员，以免错误递交投标/报价文件。

四、投标/报价人授权代表参加开标会的，应凭法定代表人证明及授权书、身份证原件进入开标会场并递交投标/报价文件。

五、请仔细检查投标/报价文件格式中应盖章、签署之处是否有按要求盖公章、签名、签署日期。投标/报价文件需签名之处必须由当事人亲笔签署，法定代表人证明及授权书需法定代表人签字或签章处，应由法定代表人亲笔签署或加盖签章。

六、采购代理机构不对供应商购买采购文件时提交的相关资料的真实性负责，如供应商发现相关资料被盗用或复制，或出现同一供应商由两名或以上授权代表报名的，应遵循法律途径解决，追究侵权者责任。对一家供应商递交两份投标/报价文件的，评委会将按采购文件中有关无效投标/报价的规定处理。

七、供应商在报名时提交了报名资料不代表其已通过资格性、符合性审查，供应商应在投标/报价文件中另行提供。

八、采购文件中要求“原件备查”、“核验原件”等情况的，均要求供应商把相应原件带至现场。

九、为了提高效率，节约社会交易成本与时间，希望购买了采购文件而决定不参加本次投标/报价的供应商，在投标/报价文件递交截止时间的3日前，按《投标/报价邀请函》中的联系方式，以书面形式告知我公司。对您的支持与配合，谨此致谢。

由于交通、天气等状况、停车位已满或电梯拥挤等原因，建议投标/报价人代表提前15-30分钟到达开标会场，我公司所处位置有多路公共交通线路到达，具体如下：

广州市东风东路555号（黄华路口）粤海集团大厦2203-2204室。主要路经的公交车有高峰快线12、高峰快线14、2、11、27、33、54、56、62、65、74、83、85、133、185、204、209、224、224A、261、283、284、289、293、305、483和B3、B4等在越秀桥站下车即可到达本公司。地铁可由一号线农讲所站或五号线小北站出站后步行约20分钟到达，地铁站与本公司距离较远，请查好路线后再选用。

（本提示内容非采购文件的组成部分，仅为善意提醒。如有不一致，以采购文件为准。）

目 录

第一章 磋商邀请函.....	3
第二章 报价人须知.....	5
第三章 采购人需求.....	12
第四章 合同.....	35
第五章 磋商细则.....	40
第六章 报价文件格式.....	49

第一章 磋商邀请函

广州群生招标代理有限公司受采购人的委托，拟对以下项目进行竞争性磋商，欢迎符合资格条件的供应商参加。

一、采购项目编号：GZQS1901FC04038

二、采购项目名称：增城日报《增城之窗门户网站》系统等级保护测评建设项目

三、采购预算：人民币 353000 元

四、采购数量：1 项

五、项目内容及需求：

增城日报《增城之窗门户网站》系统等级保护测评建设项目（详见采购人需求）。

（报价人必须对项目进行整体报价，不允许仅对其中部分内容进行报价。）

六、供应商资格：

1. 供应商必须是具有独立承担民事责任能力的在中华人民共和国境内注册的法人，报价时提交有效的企业法人营业执照（或事业法人登记证）副本复印件。

2. 营业执照经营范围具有相关内容，以工商营业执照批准的经营为准，如营业执照没有体现经营范围的，则须提供工商部门网站查询页面（含经营范围）打印件。

3. 已登记报名并获取本项目采购文件。

4. 本项目不接受联合体磋商。

（登记获取磋商文件时提供报名资料如下：（1）营业执照复印件（加盖公章，原件备查）；（2）法人代表证明及授权文件（原件，版本从 <http://www.gzqunsheng.com/>常用文件一栏下载）；（3）报名登记表（版本从 <http://www.gzqunsheng.com/>常用文件一栏下载）。）

七、符合资格的报价供应商应当在 2019 年 5 月 21 日起至 2019 年 6 月 2 日期间（办公时间内，法定节假日除外）到广州群生招标代理有限公司（详细地址：广州市东风东路 555 号粤海集团大厦 2203-2204）购买磋商文件，磋商文件每套售价 300 元（人民币），售后不退。

八、提交磋商响应文件截止时间：2019 年 6 月 3 日 14: 30，提交磋商响应文件时间：2019 年 6 月 3 日下午 14: 00 至 14: 30

九、提交磋商响应文件地点：广州市东风东路 555 号粤海集团大厦 2204

十、磋商时间：2019 年 6 月 3 日 14: 30

十一、磋商地点：广州市东风东路 555 号粤海集团大厦 2204

十二、本公告期限（3 个工作日）自 2019 年 5 月 21 日至 2019 年 5 月 23 日止。

十三、联系事项

（一）采购单位：增城日报社

地址：广州市增城区荔城街荔乡路 81 号

联系人：刘先生

联系电话：020-32821331

（二）采购代理机构：广州群生招标代理有限公司

地址：广州市越秀区东风东路 555 号粤海集团大厦

联系人：程先生

联系电话：020-83812782、83812935

传真：020-83812783

邮编：510060

电子邮箱：gzqunsheng@gzqunsheng.com

十四、本项目的所有相关公告会在中国政府采购网(www.ccgp.gov.cn)、广州市政府采购网（非政府采购）(gzg2b.gzfinance.gov.cn)和广州群生招标代理有限公司网站（www.gzqunsheng.com）上公布，公布之日即视为有效送达之日，不再另行通知。

第二章 报价人须知

1. 总体说明

1.1. 资金说明

财政性资金。

1.2. 关于限价

本项目的最高限价见第三章《采购人需求》，凡第一次报价超出最高限价的报价将被视为无效报价。

1.3. 适用范围

本项目仅适用于本磋商文件所述的报价内容。

1.4. 合格的报价人

1.4.1 具有符合磋商邀请中合格报价人资格要求；

1.4.2 已在本项目报名及购买磋商文件的报价人。

1.5. 报价人应承担所有参与本次报价的全部费用。

1.6. 合格的货物和服务

1.6.1 报价人提供的所有货物及服务，其来源均应符合相关法律法规的规定。

1.6.2 采购人将拒绝接受不合格的货物和服务。

1.7. 定义

1.7.1. “采购人”系指磋商邀请中所指采购人，亦指业主。

1.7.2. “采购代理机构”系指广州群生招标代理有限公司。

1.7.3. “报价人”系指向采购代理机构提交合格报价文件的法人。

1.7.4. “甲方”系指采购人，合同的一方当事人。

1.7.5. “乙方”系指成交供应商，合同的一方当事人。

1.7.6. “日期”指公历日，“时间”指北京时间。

1.7.7. “实质性响应”系指符合磋商文件要求、条款、条件和规定，且没有重大偏离或保留。重大偏离或保留指影响到磋商文件规定的范围、质量和性能，或限制采购人的权利和报价人的义务的规定，而纠正这些偏离将影响到其他递交实质性响应磋商文件的报价人的公平竞争地位。

1.7.8. 磋商文件中的标题或题名仅起引导作用，而不应该作为对磋商文件内容的理解或解释。

1.8. 知识产权

1.8.1. 报价人必须保证，采购人在中华人民共和国境内使用报价货物、资料、技术、服务或其任何一部分时，享有不受限制的无偿使用权，不会产生因第三方提出侵犯其专利权、商标权或其它知识产权而引起的法律或经济纠纷。如报价人不拥有相应的知识产权，则应由报价人负责获得并提供给采购人使用，其报价中必须包括合法获取该知识产权的一切相关费用，如报价人没有单独列出的，视为已包含在相应报价中。一旦使用报价人提供的产品或服务，采购人不再承担第三方提出侵犯其专利权、商标权或其它知识产权而引起的法律或经济纠纷。

1.9. 关联企业

1.9.1. 除联合体外，法定代表人或单位负责人为同一个人或者存在直接控股、管理关系的不同供应商，不得同时参加同一项目或同一子包（子项、标段等）的报价。如同时参加，则评审时将同时被拒绝。

1.9.2. 同一报价人授权不同的人员参与同一项目或同一子包（子项、标段等）的报价，则评审时将同时被拒绝。

1.10. 提供前期服务的供应商

为采购项目提供整体设计、规范编制或者项目管理、监理、检测等服务的供应商，不得再参加该采购项目的其他采购活动。

1.11. 磋商文件的解释权

本磋商文件的解释权归“广州群生招标代理有限公司”所有。

2. 磋商文件

2.1. 磋商文件的组成

- (1) 磋商邀请
- (2) 报价人须知
- (3) 采购人需求
- (4) 合同（样本）
- (5) 磋商细则
- (6) 报价文件格式

2.2. 磋商文件的澄清

2.2.1. 报价人如需澄清磋商文件的疑点，均应以书面形式加盖公章（电传、传真、电报无效）向采购代理机构提出澄清要求，通知应确保采购代理机构在报价截止日期 4 天前收到。采购代理机构

将用信函、传真等形式做出答复。

2.3. 磋商文件的补充和修改

- 2.3.1. 采购代理机构可以用书面补充通知的方式对磋商文件进行补充和修改。对磋商文件的补充和修正，将会在磋商邀请所述网站上公布，并用信函、传真等形式通知所有报价人。
- 2.3.2. 所颁发的补充通知将于报价截止期前发往所有报价人。该补充通知应作为磋商文件的一部分。报价人在收到通知后应在报价文件中予以确认。
- 2.3.3. 考虑到补充通知的影响，采购代理机构可决定延迟磋商时间。

3. 报价总则

3.1. 报价文件的编写

- 3.1.1. 报价人应仔细阅读磋商文件的所有内容，按磋商文件的要求制作并递交报价文件，并保证所提供的全部资料的真实性、准确性，以确保其对磋商文件做出实质性响应；否则，将拒绝其报价。报价人若提供不真实的材料，无论其材料是否重要，都将有可能直接导致报价无效，并承担由此产生的法律责任。
- 3.1.2. 语言和计量单位：报价文件和来往函件应用简体中文书写，报价人提供的支持文件、技术资料和印刷的文献可以用其他语言，但相应内容应附有中文翻译文本（经公证处公证），对不同文字文本报价文件的解释发生异议的，以中文文本为准。计量单位应使用国际公制单位。
- 3.1.3. 报价人应用人民币报价。报价文件的大写金额和小写金额不一致的，以大写金额为准；总价金额与按单价汇总金额不一致的，以单价金额计算结果为准；单价金额小数点有明显错位的，应以总价为准，并修改单价。
- 3.1.4. 报价人在编写报价文件时，应填写磋商文件要求的内容及其附件，并根据实际情况补充评审所需资料，报价文件只填写和提供了磋商文件要求的部分内容和附件，或没有提供磋商文件中所要求的全部资料及数据，或没有按实际情况提供报价所需资料的，其可能导致的结果和责任由报价人自行承担。
- 3.1.5. 报价人的报价明显低于其他报价，使得其报价可能低于其个别成本的，有可能影响商品质量和不能诚信履约的，应当要求该报价人作出书面说明并提供相关证明材料。报价人不能合理说明或者不能提供相关证明材料的，由磋商小组认定该报价人以低于成本报价，其报价应作无效报价处理。
- 3.1.6. 采购代理机构不接受电报、电话、电传、传真等非约定形式报价。

3.2. 报价文件的构成

报价人编写的报价文件格式详见报价文件目录表。

3.2.1. 报价人应按照磋商文件的要求编制带有目录和页码并装订成册的报价文件。

3.2.2. 报价人必须自行承担因其报价文件的任何错漏而导致的一切后果。

3.3. 报价的修改及撤回

3.3.1. 在报价截止时间前，报价人可以以书面通知的形式向采购代理机构修改或撤回其报价文件。修改后的报价文件须按照本项目规定的报价截止时间之前重新递交，否则，采购代理机构将拒绝接受修改后的报价文件。

3.3.2. 在报价截止时间后，报价人不得对其报价文件作任何修改。从报价截止时间至报价有效期满之前，报价人不允许撤回其报价文件。

4. 报价要求

4.1. 报价

4.1.1. 全部报价文件应一式五份，正本一份，副本四份，副本可由正本复印而成；报价文件电子版1份，光盘或U盘介质，WORD或EXCEL格式，不留密码，无病毒，内容应与报价人打印产生的纸质报价文件内容一致，如有不同，以纸质报价文件为准。除特别注明外，报价文件应提交纸质文件。如果正本与副本不符，应以正本为准。报价文件应由报价人的合法授权代表正式签署，如有任何更改应由原签署人签字。无论报价结果如何，报价人的全部报价文件均不退回。另按要求单独提交一个“报价信封”。

4.1.2. 报价人应对报价项目提供完整的详细的实施方案。

4.1.3. 所有报价文件应在报价截止时间前送达磋商文件指定地点，交予采购代理机构专职负责人，任何迟于这个时间的报价将被拒绝。

4.1.4. 所有报价文件必须封入密封的信封或包装，在封口上加盖报价单位公章，并在每一信封或包装的封面上写明：

（正本/副本/报价信封）	
收件人名称：广州群生招标代理有限公司	
项目编号：	项目名称：
报价人名称：	报价人地址：
联系人：	联系电话：

4.1.5. 采购代理机构不接受电报、电话、电传、传真、邮寄报价。

4.2. 报价有效期

从报价截止日起，报价有效期为 90 天。在特殊情况下，采购代理机构可于报价有效期满之前要求报价人同意延长有效期，要求与答复均应以书面形式。报价人可以拒绝上述要求而其保证金不被没收，同意延期的报价人根据原截止期所享有的权利及其所负有的义务相应也延至新的截止期。

4.3. 保证金

4.3.1. 报价人应向采购代理机构提交报价保证金人民币 10000.00 元整 保证金为人民币，报价保证金作为报价人报价的组成部分，与报价文件一同递交。

收款单位名称：广州群生招标代理有限公司

开户行：交通银行广州金迪支行

账号：441168596018800001089 (代理服务费请不要汇入此账号)

电话：020-83812782 财务联系人：喜小姐

请在银行进账单事由栏中注明“(本项目编号)”保证金。

4.3.2. 保证金一般应以报价人的名义转账，否则应出具报价人授权书。

4.3.3. 递交报价文件时请将保证金汇款声明函（加盖公章，格式详见第六章）封入“报价信封”里。

4.3.4. 如报价人未按上述规定提交保证金，其报价文件将被拒绝。

4.3.5. 在确定成交供应商后五个工作日内，无息退回未成交供应商的保证金；在签订合同后五个工作日内，无息退回成交供应商的保证金；在报价有效期内不能确定成交供应商的，在报价有效期满后五个工作日内，无息退回所有报价人的保证金。

4.3.6. 成交供应商有下列情形之一的，采购代理机构不予退还其交纳的保证金：

- (1) 报价人在参与报价活动期间，违反有关法律法规及政府采管理部门规定的；
- (2) 报价人在收到成交通知书后，在磋商文件规定的时间内无正当理由不与采购人或者采购代理机构签订合同的；
- (3) 将成交项目转让给他人，或者在报价文件中未说明，且未经采购人同意，将成交项目分包给他人的；
- (4) 拒绝履行合同义务的；
- (5) 其他违法、违规行为的。

4.3.8. 所有报价人的保证金以银行划账或电汇的方式予以退还。

5. 磋商、成交与签约

5.1. 磋商

详见《第五章 磋商细则》

5.1. 定标与签约

- 5.1.1. 评审结果确定后，如有需要，采购代理机构应通知评委会推荐的成交候选人在2个工作日内，按报价文件中所列的相关证件、证明文件、合同的原件送采购人核对与供应商响应文件中的复印件是否一致。采购人在接到原件之日起3个工作日内，核对没有不一致的，须确认成交的供应商；核对发现有不一致或供应商无正当理由不按时提供原件的，书面向采购代理机构提出，核实后按无效报价处理。
- 5.1.2. 采购人确认结果后，采购代理机构将成交结果以网上公告的方式通知所有未成交的报价人，并向成交供应商发出《成交通知书》。
- 5.1.3. 成交供应商应在规定时间内与采购人签订合同。
- 5.1.4. 在订定合同过程中，如发现成交供应商以他人名义报价或者以其他方式弄虚作假，骗取成交的，采购人有权取消其成交资格，并将第二成交候选人确定为成交供应商，依此类推。

6. 采购代理服务费用

成交单位在领取《成交通知书》之前须向采购代理机构交纳的服务费，本项目招标代理服务费为人民币8000元整。

(3) 币种与《成交通知书》的币种相同。

(4) 成交单位中标后，必须按规定向采购代理机构直接缴交采购服务费。成交单位不按规定交纳服务费的，采购代理机构将以成交单位的报价保证金抵扣服务费，不足部分采购代理机构保留进一步追索权利。

(5) 服务费不在报价中单列。

(6) 经依法取消或放弃成交资格的，采购代理服务费不予退还。

7. 询问、质疑

7.1 供应商可以向代理机构提出询问和质疑，代理机构依照相关规定就采购人委托授权范围内的事项作出答复。

7.2 供应商认为磋商文件的内容损害其权益的，可以在磋商文件公示期间或者自期满之日起7个

工作日内以书面形式向采购人或代理机构提出质疑，逾期质疑无效。

7.3 供应商在法定质疑期内须一次性提出针对同一采购程序环节的质疑。

7.4 供应商认为磋商过程和中标结果使自己的权益受到损害的，可以在知道或者应知其权益受到损害之日起7个工作日内，以书面形式向采购人或代理机构提出质疑，逾期质疑无效。

7.5 质疑函应当署名。质疑供应商为自然人的，应当由本人签字并以右手食指手指手印作为确认；质疑供应商为法人或者其他组织的，应当由法定代表人签字并加盖公章。质疑内容不得含有虚假、恶意成份。依照谁主张谁举证的原则，提出质疑者必须同时提交相关确凿的证据材料和注明证据的确切来源，证据来源必须合法，代理机构有权将质疑函转发质疑事项各关联方，请其作出解释说明。对捏造事实、滥用维权扰乱采购秩序的恶意质疑者，将上报监督管理部门依法处理。

7.6 询问及质疑函应按相应格式进行填写及签署，并递交书面文件至代理机构，没有签署的质疑函将不予受理。具体格式详见<http://www.gzqunsheng.com/>常用文件一栏。

7.7 询问、质疑受理单位：广州群生招标代理有限公司，联系电话：(020) 83812782。

第三章 采购人需求

一、项目概述

增城日报是增城区《增城之窗门户网站》的建设和管理单位，该平台承载我区所有信息发布业务系统

现增城之窗门户网站运行的各类信息包含《数字报》、《手机报》、政务、商业等信息系统等，这些网站和系统是履行职能、面向社会提供服务的窗口，是实现政务信息公开、服务企业和社会公众、方便公众参与的重要渠道，同时也是对外宣传政府形象、发布行业信息，是增城区重要信息系统之一。

增城区增城日报是增城区《增城之窗门户网站》网站的载体，作为社会公众获取政府信息和服务的主要接入渠道和信息发布平台，自然成为信息安全防护体系中重要组成部分，受到公安等相关部门的高度重视。然而在平台的实际运行过程中，安全问题由其重要，常规的物理安全防护手段无法进行有效保护，需要根据网络安全法，需针对网站要求进行安全等级保护测评与整改。

本项目最高限价为人民币 353000 元。

序号	服务内容	期限 (年)	数量	最高限价（元）
1	信息系统等级保护测评服务：定测评机构进行测评	/	一项	50000
2	信息系统等级保护测评整改服务费：针对等保测评不符合子项进行整改	/	一项	118000
3	信息系统迁移服务：迁移服务	/	一项	27500
4	云平台租赁	1	1	97500
5	互联网出口：广州市信息化服务中心互联网出口	1	2	30000*2=60000
合计				353000 元

二、项目建设目标、规模、周期

项目建设目标：增城日报社《增城之窗门户网站》网站信息系统提供二等级保护标准环境，建立基本的安全防护措施，提高网络信息系统整体主动防御功能，确保信息应用系统能满足日后的快速发展需求。

项目建设规模：一个网站系统的迁移、等保二级过级。

项目建设周期：一年。

三、经济及社会效益

1、投资效益：

降低总体拥有成本（TCO）、提高投资回报率（ROI）；降低运营和维护成本，包括数据中心空间、

机柜、网线，耗电量，冷气空调和人力成本等。

2、安全效益：

系统安全性：

由于采用了虚拟化技术的高级功能，使业务系统脱离了单台物理硬件的束缚，可以实现更高级别的业务连续性要求，提升了系统安全性、可靠性。

通过虚拟化技术，降低了物理硬件的故障影响力，减少了硬件的安全隐患。

通过虚拟化整合，减少了设备的接入数量，安全防范的范围能够得到更有效地控制。

可为用户提供定制化安全服务，如安全等保类服务。

3、服务效益：

提高服务水平：

帮助企业建立业务和 IT 资源之间的关系，使 IT 和业务优先级对应。

将作为统一资源池进行管理，并按需进行资源调配，快速响应业务部门提出的系统资源需求。

4、投资保护效益：

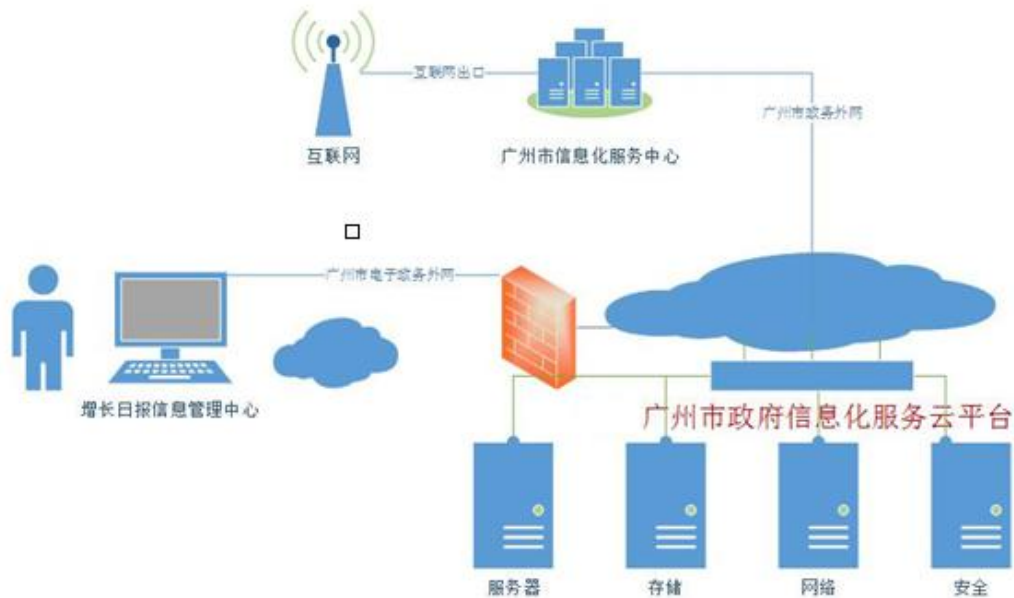
虚拟化平台具有更广泛的操作系统（OS）兼容性，不再担心旧系统的无法使用，并且通过自动更新功能实现维护和升级等一系列问题。

四、业务上云项目内容

（一）云业务上云

根据用户现有的应用系统运行环境，通过在云上搭建等同或优于现有的应用运行环境的云主机平台，将增城《增城之窗门户网站》的应用系统迁移至云上。

（二）云连接拓扑图



(三) 业务上云迁移

1、业务迁移总体思路：

增城《增城之窗门户网站》应用在迁移前做好数据备份，迁移的业务系统提前告知各个部门，以免出现不必要的问题。

迁移前做好迁移测试演练，处理迁移过程中出现的各种故障，保障正式迁移避免一切故障。使迁移顺利。

迁移完成后进行业务系统的完整性测试，这些测试包括但不限于数据一致性测试、数据完整性测试、应用会话状态完整性测试、连接中断测试、数据恢复测试。只有这样才能保证迁移的安全性和有效性。

2、迁移步骤设计：

增城《增城之窗门户网站》应用架构情况采用专业工具，将业务系统进行转化，使其符合云平台可识别的业务系统。

技术人员将转换后的业务系统平滑迁移至云。

增城《增城之窗门户网站》应用系统迁移完成后，进行相关功能性测试，保障业务系统的完整性。

3、迁移规划设计：

(1) 前期部署：

首先在工作机和云主机上安装 **node** 软件，控制机上安装控制机软件。如有防火墙，则根据以下端口列表作相应的开放设置；

	端口	协议	端口号	作用
工作机	RPC 服务端口	tcp	26821	控制机->工作机
	恢复端口	tcp	26831	灾备机->工作机
云主机	RPC 服务端口	tcp	26822	控制机->灾备机
	镜像端口	tcp	26832	工作机->灾备机
	复制端口	tcp	26833	工作机->灾备机
控制机	HTTP 端口	tcp	58080	HTTP 端口
	HTTPS 端口	tcp	55443	HTTPS 端口

(2) 服务器迁移：

服务器迁移主要用于全服务器保护，即，可以将主机的网络、数据、系统状态全部备份到备机，如果需要，用户可以手动从主机切换到云主机，从而实现服务器的迁移。

(四) 广州市政府信息化云服务平台

1、服务提供能力

广州市政府信息化云服务平台面向政府客户提供云化的 IT 基础设施，包括但不限于

(1) 云平台 IaaS 服务：计算即服务、存储即服务、网络即服务、机房服务。

(2) 云平台 PaaS 服务：数据库即服务、中间件即服务、测试即服务、操作系统服务（云服务市场：移动应用支撑服务、业务应用组件服务、大数据服务）。

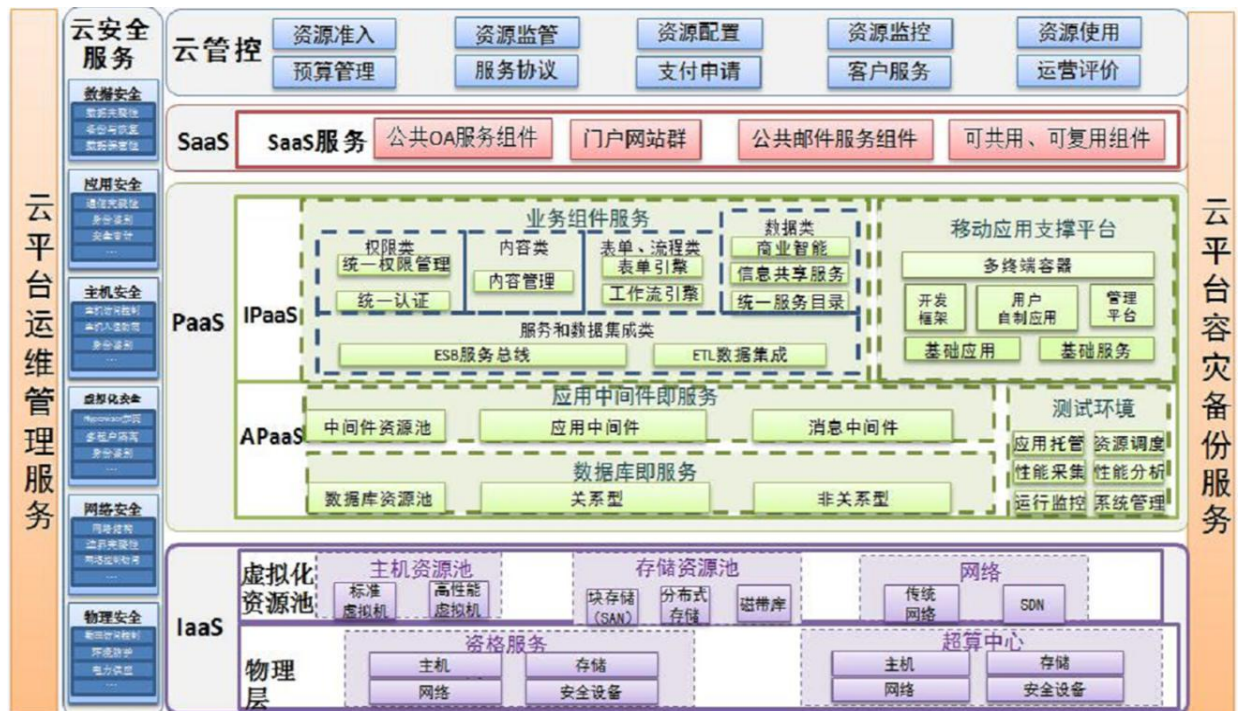
(3) 云资源管理平台：云服务管控平台由广州市信息化服务中心建设，我方所建设云资源管理平台与云服务管控平台实现对接。

(4) 容灾备份服务：各使用单位应用系统提供本地及同城异地的数据备份和恢复的能力。我方容灾云平台。

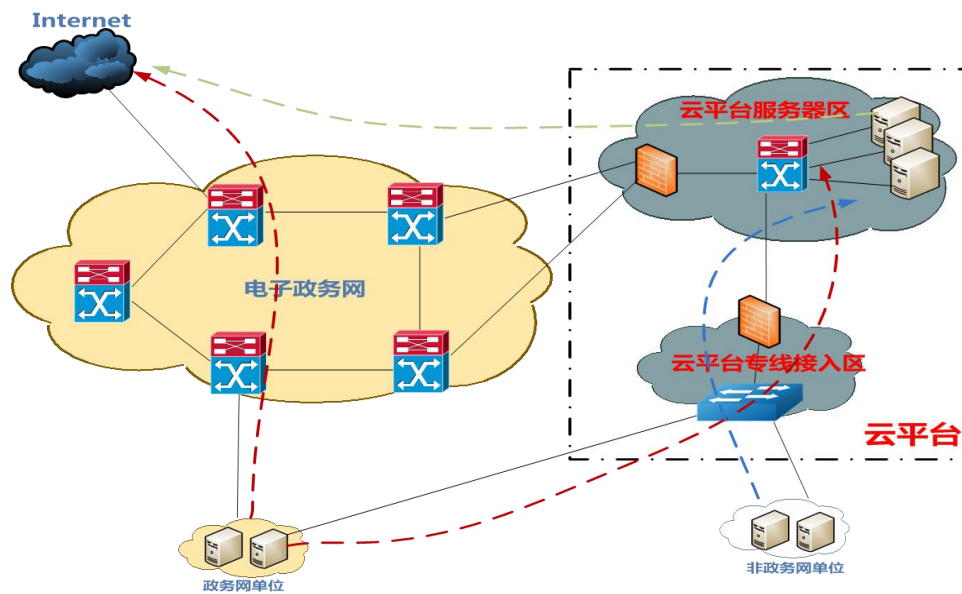
(5) 信息安全服务：提供云资源二级等保支持服务。提供增值安全服务，至少具备达到等级保护三级的安全资源和服务能力，以供使用单位选择使用。

基础设施即服务		平台即服务			安全即服务							
计算即服务	小型虚拟机	数据库即服务 (含技术服务)	关系型数据库	RDS单实例版服务	虚拟化安全服务	虚拟防火墙服务	向租户提供虚拟防火墙及入侵防御服务					
	中型虚拟机			RDS HA版服务	主机安全服务	主机漏洞检测服务	向租户提供按需计费的在线漏洞检测服务					
	大型虚拟机			HA版		主机防病毒服务	向租户提供主机防病毒应用软件					
	定制化虚拟机服务			vCPU	应用集群版	应用层防火墙	向租户提供虚拟化WAF设备					
	物理服务器	高负载数据库服务器1	大数据服务	数据仓库(云服务市场)	Web安全防护	WEB防篡改服务	向租户提供网站防篡改应用软件					
						内存	非关系型数据库	WEB漏洞检测服务(云服务市场)	向租户提供按需计费的在线WEB漏洞检测服务			
		高负载数据库服务器2				中间件即服务 (含技术服务)		开源中间件服务	向租户提供WEB监测客户端软件			
							商业中间件服务	WEB监测服务(云服务市场)	向租户提供在线WEB网站监测服务			
		2U机柜				基础软件	数据库许可及技术支持服务 开源中间件售后服务 Linux 服务器版授权及服务支持 Windows技术支持	安全运维管理服务	基线核查服务(云服务市场)	向租户提供按需计费的在线基线核查服务		
		小型机托管服务				测试即服务	测试环境服务	安全测评和审计服务	数据库审计服务(云服务市场)	向租户提供虚拟化数据库审计设备加服务		
GPU服务1	业务组件服务	统一权限管理(云服务市场)	系统源代码检测服务(云服务市场)	向租户提供按需计费的系统源代码检测服务								
GPU服务2		统一认证(云服务市场)	系统上线安全测评(云服务市场)	向租户提供按需计费的系统上线安全测评服务								
GPU服务3		内容管理(云服务市场)	APP安全服务(云服务市场)	APP安全服务(云服务市场)	向租户提供按需计费的APP检测服务							
GPU服务4		表单引擎(云服务市场)		密码服务	虚拟密码机VSM(云服务市场)	向租户提供部署在虚拟机上的增强VSM						
分布式文件存储	FC-SAN	工作流引擎(云服务市场)	安全即服务				数据级容灾服务	应用双活容灾服务(云服务市场)				
		商业智能(云服务市场)		移动应用支撑服务	ESB服务总线(云服务市场)	向租户提供部署在虚拟机上的基础VSM						
		信息共享服务(云服务市场)							ETL数据集成(云服务市场)	向租户提供部署在虚拟机上的增强VSM		
		统一服务目录(云服务市场)									移动应用支撑服务	企业移动化管理平台(云服务市场)
基础备份服务能力	虚拟磁带库或备份一体机	移动应用支撑服务	企业移动化管理平台(云服务市场)				企业移动终端、PC终端(云服务市场)					
同城备份服务能力	虚拟磁带库或备份一体机			移动应用支撑服务	企业移动化管理平台(云服务市场)	企业移动终端、PC终端(云服务市场)						
备份能力堆叠	虚拟磁带库或备份一体机							移动应用支撑服务	企业移动化管理平台(云服务市场)	企业移动终端、PC终端(云服务市场)		
											磁带库	移动应用支撑服务
网络即服务	负载均衡服务	硬件级负载均衡	软件级负载均衡				容灾即服务				数据级容灾服务	

2、平台系统架构：



3、云平台基础网络架构：



4、云平台安全服务方案：

(1) 基础安全服务方案

建设的云平台安全服务包括但不限于如下：机房安全、网络安全、主机安全、云管理平台安全等。

① 机房安全：建设云服务中心的机房需满足国家 A 级（GB50174-2008）的安全要求。

② 网络安全：针对云平台建立一套网络安全防护体系，对网络边界处提供访问控制、病毒过滤、防攻击、防入侵、防篡改、内外网数据安全隔离交换等立体安全防护，保护应用系统和内/外网计算机安全。

◆访问控制：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。通过网络及安全系统的部署具备限制网络最大流量数及网络连接数的功能，在网络中的各个应用层面实现对各网段的防止地址欺骗控制，支持按用户和系统之间的允许访问规则，允许或拒绝用户对受控系统进行资源访问，控制粒度为单个用户，同时通过 VPN 网关及软件系统应用功能实现对远程拨号访问权限的用户数量进行限制。

◆安全审计：对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告，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：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包括：端口扫描、强力攻击、木马后门攻击、拒绝服务攻击、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：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：所使用的网络设备均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具备唯一标识。

③主机安全：对主机的物理安全摆放位置，主机访问控制方面进行保护。

◆主机访问控制：主机系统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。

◆堡垒机：通过堡垒机进行统一的账户管理、统一认证，以及对运维的会话命令等进行审计、对权限进行精细化控制等，从而实现身份管理、访问控制、权限控制、操作审计等功能。

④云管理平台安全：包括虚拟化及云管理平台的安全保护。

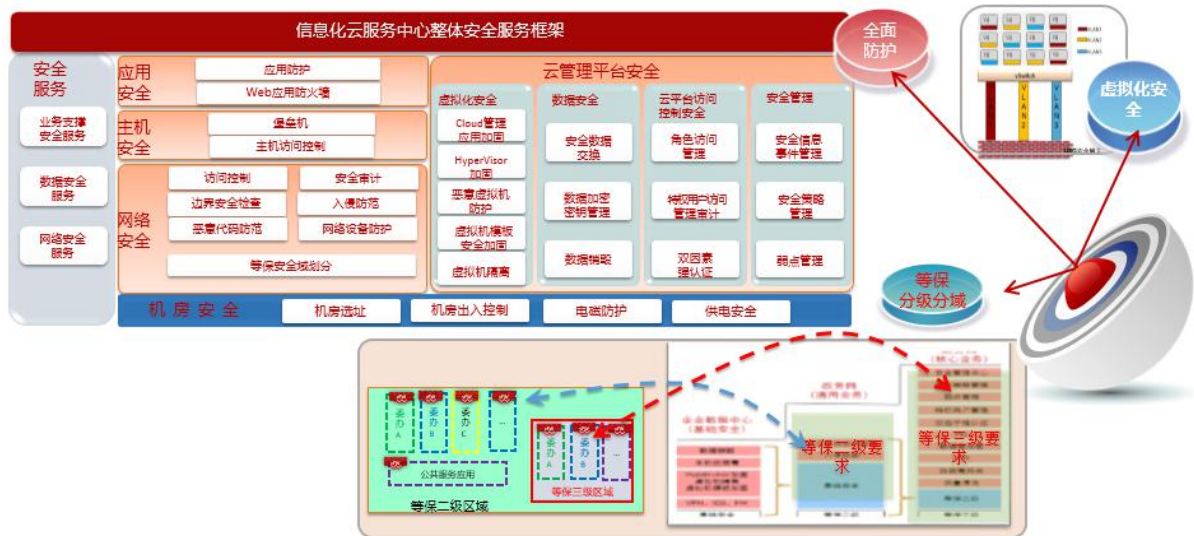
◆虚拟化安全：支持有代理或者无代理安全方式进行虚拟环境的整体防护；支持对关闭的虚拟机/模板进行安全扫描和防护，防止关闭状态的虚拟机/模板的安全策略/补丁更新不及时过期出现安全隐患；整体的虚拟化安全措施应避免“病毒风暴”。

◆云平台安全：如果云管理平台需要数据库的支持，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。

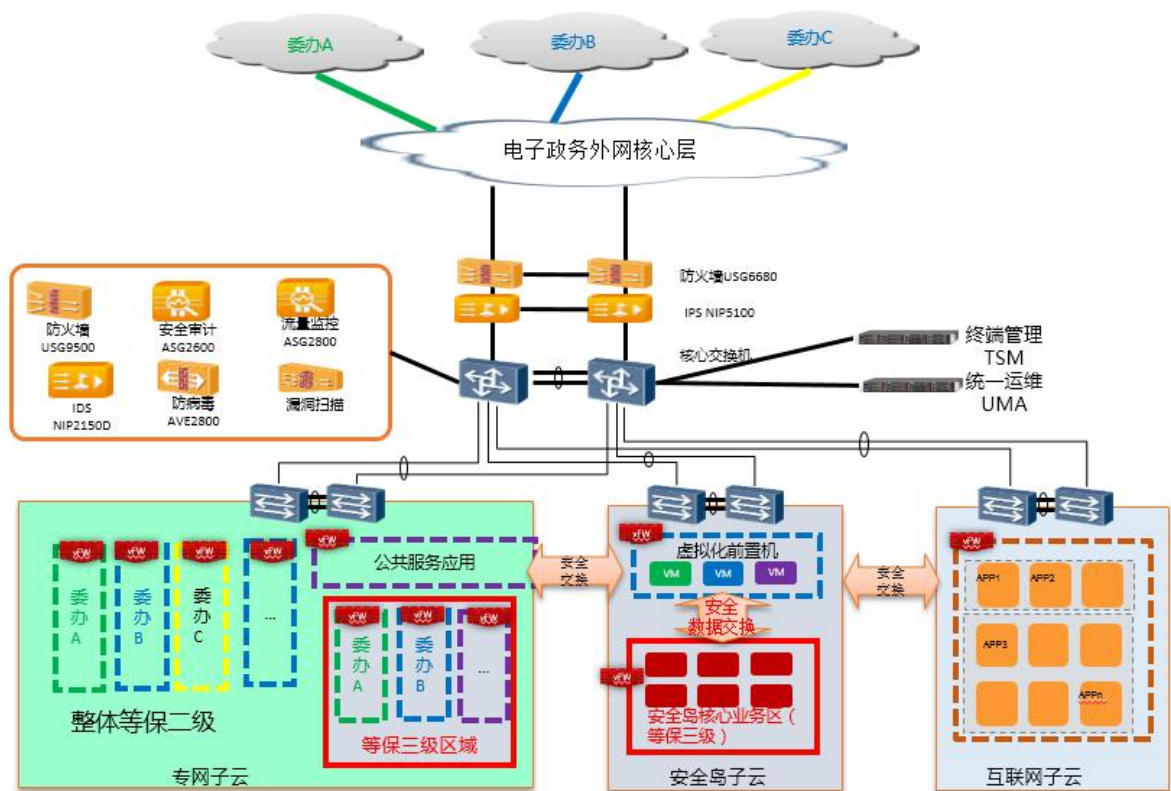
◆云平台访问控制安全：用户在访问云平台资源过程中支持使用数字证书进行身份认证，包括但不限于维护人员、使用单位操作人员、市信息化服务中心监管人员，且数字证书的介质购买和服务费由成交供应商提供。

◆各使用单位部署在云平台中的应用系统运行的过程中，若发现重大安全事故或者安全隐患时，成交供应商配合进行安全整改。

(2) 云平台安全服务设计框架：



(3) 云平台安全拓扑图：



①全面防护，符合平台规范和等保要求：

- a、网络安全：完整的边界和内部安全防护方案
- b、主机安全：部署终端安全设备，实现主机安全加固
- c、云管理平台安全：全系列安全设备虚拟化，实现“委办局”定制化安全服务

②等保分级分域，针对等保三级区域安全加固

- a、云平台整体满足等保三级要求，
- b、全面的安全监测和审计，满足政府监管要求

③可信数据集中共享交换

“vFW+VM 前置机”部署：快速实现安全数据共享交换

④提供高性能安全设备提供大数据流量下安全防护能力，保证平台可平滑扩容

(4) 机房安全设计：

● 机房选址

机房和办公场地选择在具有防震、防风和防雨等能力的建筑内。机房场地应避免设在建筑物的高层或地下室，以及用水设备的下层或隔壁。

● 机房管理

机房出入口安排专人值守，控制、鉴别和记录进入的人员；

需进入机房的来访人员须经过申请和审批流程，并限制和监控其活动范围。

对机房划分区域进行管理，区域和区域之间设置物理隔离装置，在重要区域前设置交付或安装等过渡区域；

重要区域应配置电子门禁系统，控制、鉴别和记录进入的人员。

● 机房环境

合理规划设备安装位置，应预留足够的空间作安装、维护及操作之用。房间装修必需使用阻燃材料，耐火等级符合国家相关标准规定。机房门大小应满足系统设备安装时运输需要。机房墙壁及天花板应进行表面处理，防止尘埃脱落，机房应安装防静电活动地板。

(5) 网络安全设计：

通过在云平台出口部署防火墙、流量监控、漏洞扫描、防入侵、防篡改等安全防护设备，建立起一套完整的网络安全防护体系，对网络边界处提供访问控制、病毒过滤、防攻击、防入侵、防篡改、内外网数据安全隔离交换等立体安全防护，保护应用系统和电子政务网计算机安全。

网络安全方案提供如下能力：

● 访问控制

在云平台各网络边界处均部署安全访问控制设备，包括防火墙、IPS、VPN 网关等，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，同时安全网关和 IPS 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。

在防火墙上部署针对用户的限流和限连接，防止恶意攻击和流量非法滥用。在防火墙上开启 IP 加 MAC 绑定实现对各网段的地址欺骗控制，支持按用户和系统之间的允许访问规则，允许或拒绝用户对受控系统进行资源访问。

对于出差和远程办公通过 SSL VPN, IPSEC 连接的用户在防火墙上开启 VPN 功能,实现对远程拨号访问用户的接入，并开启对接入用户数量限制的功能。

● 安全审计

通过安全管理设备 ASG，可对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，并能够根据记录数据进行分析并生成审计报告，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

方案通过部署网络行为管理系统、安全审计系统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

在云平台出口部署 IDS 和 IPS 入侵防范、检测系统等安全网关系统，实现的实时防范功能。包括：端口扫描、强力攻击、木马后门攻击、拒绝服务攻击、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

在网络的边界部署恶意代码检测分析工具 AVE，并自动对恶意代码库的升级和检测，实现对恶意代码的防护。

● 网络设备防护

采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，并可通过命令行、Web、中文图形化配置软件等方式进行配置和管理，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都具备唯一标识。

● 日志搜集分析

对 NAT 日志、URL 访问记录、IM 上下线的日志记录，以及针对 P2P、游戏等低价值流量的必要控制，确保政务云正常业务的访问体验。

（6）云平台主机安全：

①虚拟化平台安全：

数据中心虚拟化安全解决方案，可以实现对于数据中心中各“安全域”内的所有资源使用“安全域”对应的统一安全策略进行管理与防护，管理员无需在使用中对其中的物理计算机、物理网络资源、虚拟计算机、虚拟网络区别对待，只需根据资源的安全属性与功能统一设置安全策略，最大程度保证虚拟化安全与传统安全技术与策略的归一性，以及数据中心不同租户、不同功能实体之间管理责权的划定。

虚拟化安全方案需要提供如下功能：

● Vswitch 侧流量控制与监测

vSwitch 与 vNIC 之间的流量，包括需要和不需要出入主机的流量都要进行控制与监测。

● VM 之间流量控制与监测

不同的 VM 往往部署不同的业务功能，因此需要对 VM 之间（包括同一主机和不同主机上的 VM）的流量进行控制与监测。在相同租户，相同虚拟网段内，可根据不同的安全策略在虚拟机之间划分不同的“安全域”，并实现通信隔离以及网络通信安全控制功能；

● VM 安全状态监测

本次业务平台云计算资源池中大量的 VM 可能被随时启动或者关闭，也可能随时产生变化，而这种变化的触发的一种可能就是由于安全问题的出现而引发的，例如某些入侵手段的一个初始动作就是监测系统里面的防病毒软件，一旦发现有防病毒软件的存在，入侵者或者工具将首先关闭它，然后才会进行后续的恶意动作，而这些问题如果能够得到监控将大大提升系统的安全防护能力。

● 支持虚拟机迁移

虚拟机迁移后需要保障安全策略一致性。

● 便捷部署与管理

虚拟化计算下，大量 VM 可以快速被创建，也可以随时被关闭。因此要求轻量级虚拟防火墙设备可以与 VM 同步，能便捷快速的部署和管理。

● 灵活的策略控制

不同的业务需求，安全策略往往不一致，同一种业务在不同时段安全策略也可能不相同。因此要求能够支持灵活的策略控制。

● 实体安全控制与虚拟安全控制的协作

虚拟环境同样构筑于实体物理环境之上，除了虚拟环境拥有其特有的安全问题之外，实体

物理环境中的安全问题也同样存在，因此，虚拟化安全控制需要能与实体安全控制协作，两者有效结合达到整体防御的成效。

●可扩展性保障

虚拟化安全解决方案对数据中的传统安全环境与虚拟化环境提供统一的安全保障框架。虚拟化防火墙等设备通过“多实例”、负载均衡、嵌入虚拟化网络等技术，可以跟随政务云数据中心在租户数量、系统规模、业务复杂性不断增加时保证安全能力的跟随扩展性。

②云平台防病毒：

云管理节点、管理终端的防病毒，整个网络的 Linux、window 防病毒集中管理和维护。

业务节点采用定制的 OS，并进行加固，安全性已经比较高，同时考虑到性能，不部署防病毒软件。

管理节点、Portal：部署基于 Linux 的 AV。

管理终端：部署基于 Windows 的 AV。

对于信息化云服务平台内的 Windows 与 Linux 服务器，使用委办局级病毒防护产品来进行集中管理和监控。

(7) 提升增值安全服务方案：

本项目的提升增值安全服务内容如下：

虚拟化安全服务：虚拟防火墙安全服务

主机安全服务：主机漏洞检测服务

应用安全服务：云 WAF 服务、WEB 防篡改服务

数据安全服务：WEB 防篡改服务、主机漏洞检测服务、虚拟防火墙安全服务

①增值安全设计原则：

云平台增值安全以面向广州市各单位、政务用户甚至是企事业单位提供安全服务为主要目标，对于当前的电子政务网络现状，基于云平台新建安全服务资源池建设需要满足以下需求。

采用 B/S 模式访问系统

增值安全服务使用采用浏览器/服务端（B/S 模式）访问系统，减少用户对系统安装维护的工作量；用户使用简单、培训容易、易扩展、支持安全服务动态感知；

采用 SOA 架构

云平台增值安全服务涉及众多单位和用户。为使各安全服务数据能够统一管理，实现与云平台系统、云平台网络融合集成，同时能够使安全服务能够快速地构建和易于扩展。系统采用 SOA 架构，把云安全服务资源池各增值安全服务按照不同需求进行分类管理。不同用户可以根据服务需求简单明了

地获取相关服务。

基于云安全服务资源池高可用架构

安全服务是一个相对动态的交付服务，需求和负载随着用户需求而变换，因此需要底层架构能实现灵活的扩展，以应对变化的需求。

另外由于安全服务厂家产品具有异构性，因此需要以相对标准且通用的底层架构来实现不同厂家的部署兼容。

独立专用管控的网络资源

安全服务涉及到如网络扫描、检测、安全策略定制等，特别是安全策略定制和开拓流程和周期相对较久，因此云安全资源池需要有专用的接入网络，并且根据提供的安全服务开放相应的安全策略以及互联网访问等权限。

安全资源池应规划日志服务器、工具资源池、测试服务器和生产设备 IP 地址段，通过防火墙进行资源的访问和管控。制定日志服务器、工具资源池、测试服务器和生产设备间策略和映射规则。限制测试服务器对生产设备（含服务器和工具资源池设备、各单位生产服务器）。

实现服务资源负载均衡

由于当前的电子政务网络分为多个网络节点，不同节点之间的网络边界划分明确，且有各自的安全管理和策略规定，为了减少节点之间流量交互以及避免安全策略管理混乱，安全资源池在每个节点分别部署，彼此之间互为主备，即满足负载需求又提高效率。

②增值安全技术实现：

在云平台内部统一规划构建安全资源池为各委办局提供虚拟化防火墙服务、主机漏洞检测服务、web 应用防护服务、web 防篡改服务、主机防病毒服务等增值安全服务，同时资源池可根据用户需求动态进行资源调控，同时提供各类服务必要的防护日志分析存储及分析功能。

资源层实现

云安全资源池是通过部署硬件安全工具、虚拟服务器构建支撑分析平台共同实现的。云安全资源池云服务使用情况如下：

◆虚拟防火墙服务：用户通过虚拟机部署软件来实现网络防护功能，此服务包括虚拟防火墙镜像软件包，虚拟防火墙镜像包实现单位业务网段网络安全防护功能。单位虚拟防火墙部署测试成功后，单位的网络管理员可根据业务需求进行防护策略配置。虚拟防火墙分析流经的网络流量，流量行为通过各种日志形式记录下来，传输到指定的日志分析系统，经日志分析系统分析结果至云管理平台，该服务实现的是传统三层防火墙和入侵防御系统的功能。用户需向根据自身需求申请虚拟机资源、日志分析系统占用空间，由云平台配置好策略后，即可自行管理虚拟防火墙和运维工作。

◆Web 防篡改服务：用户使用一台虚拟服务器作为内容发布服务器，同时业务服务器安装客户端软件包实现 web 防篡改服务功能。单位防篡改服务部署完后，业务服务器客户端软件比对服务器上的被申请访问的页面，通过比对发布服务器上备份的网站代码文件识别是否存在篡改。存在防篡改的行为会被记录并将篡改的页面进行恢复。单位防篡改服务需将事件日志对接到资源池的日志服务器（位于云管理平台同一网段）。Web 防篡改软件由单位用户运维，发生异常超出处理能力的问题由服务商提供技术支持，定期服务商对防篡改软件运行进行巡检和应急处置。

◆Web 应用防护服务：云安全资源池以硬件形式通过在云平台部署应用防火墙对用户应用防护服务，或通过 DNS 引流方式对用户应用防火墙服务。Web 应用防护服务部署完后，单位用户可自行根据业务需求在分配的应用层防火墙进行策略配置，提供支撑的专用资源池分配单位所需的应用层防火墙。应用层防火墙对恶意行为进行拦截，并将发现的事件对接到云管理平台供单位用户查询。云服务使用期间设备异常由云平台来提供技术支持和应急服务，云服务支撑的设备由使用单位进行运维。

◆主机漏洞检测服务：云服务资源池通过部署专业主机漏扫设备提供主机漏洞检测服务。单位只需提供主机漏洞检测所需信息在开通用户端策略后，云平台通过调用主机漏扫设备对单位申请漏洞的主机进行扫描检测。

◆主机防病毒服务：通过云服务资源池部署服务器提供主机防病毒服务，单位用户端通过软件形式在每台业务服务器上部署。单位业务服务器部署完防病毒客户端，经测试和试运行结束后，防病毒客户端实现主机恶意代码检测/监测，通过资源池中的扫描服务器在计划时段对服务器进行病毒检测，资源池服务器端定期下发病毒库、更新程序和定制的病毒防护策略。

网络层实现

云平台对云安全资源池规划 2 个 C 类 IP 地址段，云服务支撑工具使用一个 C 类网段，云服务所需日志分析设备或服务器使用一个 C 类网段，提供对政务云以外单位安全监测/检测需求。

策略配置规则

序号	云服务名	访问路径		目的端口	协议	单/双向
		源 IP	目的 IP			
1	主机漏洞检测服务	云管理平台服务器 IP	安全资源池漏洞检测工具 IP	8890	TCP	单向

序号	云服务名	访问路径		目的端口	协	单/	
		安全资源池漏洞检测工具 IP		单位业务服务器 IP	全通（扫描数据流经过防火墙，需白名单添加设备 IP-安全资源池漏洞检测工具 IP）		
2	防病毒服务	VPN 接入地址段		安全资源池防病毒服务器 IP 云平台服务器 IP	29443、443	TCP	单向
		安全资源池防病毒服务器 IP		服务商升级节点 IP	80	TCP	单向
		安全资源池防病毒服务器 IP		单位安装防病毒的服务器	TCP: 1688—1689、1976—1983、3306、 5557、29037、29080、29121 UDP: 7273-7282	TCP UDP	双向
		安全资源池防病毒服务器 IP		单位安装防病毒的服务器	29088	TCP	双向
3	虚拟防火墙和入侵防御系统	安全审计平台业务口 IP	单位虚拟防火墙上联口 IP	ping	TCP	双向	
4	应用防火墙服务	云平台核心交换机镜像口 IP（互联口 IP1）	云安全服务平台（互联口 IP2）	全通		双向	

序	云服务名	访问路径		目的端口	协	单/
5	web 网页 防篡改服 务	单位的发布服务 器 IP	云平台日志 服务器	514	UDP	单 向

② 增值安全技术实现：

◆ 虚拟防火墙服务

提供虚拟化网络安全服务，包括但不限于虚拟化防火墙、入侵防御等，能够满足使用单位对虚拟资源的访问控制以及边界防护等需求。

用途：虚拟化网络安全服务	
指标项	指标（除特别说明外，以下为单个实例的配置）
交付模式	虚拟机形式交付，支持 KVM、Openstack、AWS 或 Vmware ESXi 等主流虚拟化平台
部署模式	支持透明、路由、混合、旁路、直连（虚拟线）五种工作模式
使用方式	云平台安全管理接口、虚拟设备管理接口
标准防火墙规格	1、虚拟机配置：1 个 CPU、1G 内存、20G 硬盘 2、防火墙最大吞吐量：2Gbps 3、IPsecVPN 数量：50 个 4、VPN 最大吞吐量：200Mbps 5、SSL VPN 用户数:250 6、最大并发会话数:500K 7、每秒新建连接数:20K
防火墙功能	1、支持 NAT，包括动态和静态地址转换 2、支持各类主流路由协议，等价路由、策略路由 3、ALG 支持 DNS、H.323、SIP、FTP、TFTP、RSH、RTSP、SQL Net、HTTP、MS-RPC、PPTP/GRE、SUN-RPC 等应用 4、支持抵御所列所有攻击类型，包括：DNS Query Flood、SYN Flood、UDP Flood、ICMP Flood、Ping of Death、Smurf、WinNuke，动作支持记录、阻断两种模式 5、支持 GRE 和 GRE over IPSec，IPSec VPN、SSL VPN、L2TP

用途：虚拟化网络安全服务	
指标项	指标（除特别说明外，以下为单个实例的配置）
	VPN 6、支持多种算法的服务器负载均衡，支持使用 ping、应用端口等方式探测服务器状态 7、支持流量管理功能
入侵防御功能	1、支持基于状态、精准的高性能攻击检测和防御 2、支持实时攻击源阻断、IP 屏蔽、攻击事件记录 3、支持针对 HTTP、SMTP、IMAP、POP3、VOIP、NETBIOS 等 20 余种协议和应用的攻击检测和防御 4、支持缓冲区溢出、SQL 注入和跨站脚本攻击的检测和防护 5、支持专业的 Web Server 防护功能，含 CC 攻击防护和外链防护等 6、支持对 telnet、SMTP、FTP 协议的暴力破解防护 7、提供多种特征的攻击检测和防御，特征库支持网络实时更新
安全策略	1、支持基于策略或者安全域的入侵防范，可针对不同的服务器对象定制不同的规则集合 2、支持自定义入侵防御特征 3、提供预定义防御配置模板

◆ 主机漏洞检测服务

提供高效、全方位的资产安全检测服务，协助用户检测网络中的各类脆弱性风险，提供专业、有效的安全分析和修补建议，并贴合安全管理流程对修补效果进行审计，最大程度减小受攻击面。

用途：虚拟主机安全服务（漏洞检测服务）	
指标项	指标（除特别说明外，以下为单台设备的配置）
交付模式	(一) 服务方式交付（可选）
部署模式	旁路
使用方式	云平台安全管理接口、虚拟设备管理接口

规格参数	<ol style="list-style-type: none"> 1、 支持分布式部署和集中管理 2、 支持二次开发接口 3、 支持 Ipv6 环境 4、 支持仪表盘、报表展示 5、 支持告警管理 6、 支持多用户，权限控制 7、 支持资产管理 8、 检测漏洞数：大于 15000 9、 检测配置检查项数：大于 2000 10、 扫描 ip 限制：无限
功能	<ol style="list-style-type: none"> 1、 能够全面发现信息系统存在的各种脆弱性问题，包括安全漏洞、安全配置问题、应用系统安全漏洞，检查系统存在的弱口令，收集系统不必要开放的账号、服务、端口，形成整体安全风险报告 2、 能够快速定位风险类型、区域、严重程度，直观展示安全风险 3、 能够结合安全管理制度，支持安全风险预警、检查、分级管理、修复、审计流程，并监督流程的执行 4、 能够提供多种灵活部署方式，适应复杂的网络环境下的部署，并尽量控制降低安全建设成本 5、 能够在 IPv6 环境中部署和检测脆弱性
漏洞/知识库升级	支持手动升级和自动升级，支持本地升级和在线升级，在线升级支持代理方式升级
报告	支持分析报告输出

◆ 云 WAF 服务

满足对来自 Web 应用程序客户端的各类请求进行内容检测和验证，确保其安全性与合法性，对非法的请求予以实时阻断，从而对各类网站站点进行有效防护。

用途：WEB 应用安全（云 WAF）	
指标项	指标（除特别说明外，以下为单台设备的配置）

用途：WEB 应用安全（云 WAF）	
指标项	指标（除特别说明外，以下为单台设备的配置）
交付模式	虚拟机形式交付，支持 KVM、Openstack、AWS 或 Vmware ESXi 等主流虚拟化平台
部署模式	支持代理、路由牵引等模式
使用方式	云平台安全管理接口、虚拟设备管理接口
规格描述	<ol style="list-style-type: none"> 1、支持虚拟化部署 2、Web 攻击检测特征数不少于 3000 条 3、支持检测和防御 OWASP 定义 10 大 web 安全威胁（如 SQL 注入防护、XSS 攻击防护、CSRF 攻击防护） 4、支持对常见 Web 建站内容管理系统的防护，所支持的 CMS 类型数量不少 20 种 5、支持仪表盘、报表展示 6、支持告警管理 7、支持多用户，权限控制 8、支持站点管理
防御功能	<ol style="list-style-type: none"> 1、支持识别恶意请求含：跨站脚本(XSS)、注入式攻击（包括 SQL 注入、命令注入、Cookie 注入等）、跨站请求伪造等应用攻击行为； 2、支持识别服务端响应内容导致的缺陷：敏感信息泄露、已有的网页后门、错误配置、目录浏览等缺陷； 3、支持基于访问行为特征进行分析，能识别盗链、爬虫攻击的能力； 4、支持识别网站中的网页木马程序，通过策略可防止木马网页被用户访问； 5、内置主流 Webshell 特征库，对上传内容进行检查，防止恶意 Weshell 上传； 6、支持丰富的自定义规则，可以针对多个条件组合，形成深度的 WEB 防护规则

用途：WEB 应用安全（云 WAF）	
指标项	指标（除特别说明外，以下为单台设备的配置）
	7、支持服务器隐藏； 8、可配置删除服务器响应头信息； 9、支持 Cookie 安全机制，支持 Cookie 自学习； 10、支持 Cookie Httponly； 11、支持 Cookie 防篡改、防劫持。
CC 防护	1、支持访问速率和访问集中度检测算法； 2、支持 HTTP 头部多种条件匹配； 3、检测 IP 对象支持 NAT 前地址，并支持自定义检测字段功能； 4、支持挑战模式，WAF 发起 js 挑战验证； 5、支持学习业务流量模型，按需开启 CC 防护； 6、支持基于地理位置的识别，可设置不同地理位置的检测单元。

◆ WEB 防篡改服务

网页防篡改服务，满足实时监测网站的内容变更状态，发现篡改事件后及时告警和修复，降低租户的影响和减少损失。

用途：WEB 应用安全（防篡改服务）	
指标项	指标（除特别说明外，以下为单台设备的配置）
交付模式	软件产品交付
规格	1、产品（系统）形态：软件 2、完整性检查：HMAC 安全散列算法 3、传输协议：SSL 安全协议 4、安全接口：PKCS#11 安全应用接口 5、操作系统的支持：支持 WindowsServer、HP-Uinx、IBMAIX、Solaris、SuSELinux、RadHatLinux、Unix 等主流的操作平台 6、WEB 服务器的支持：支持 IIS、Apache、Nginx、J2EE（Tomcat/Weblogic/Websphere）等

用途：WEB 应用安全（防篡改服务）	
指标项	指标（除特别说明外，以下为单台设备的配置）
	7、管理方式：支持 B/S 和 C/S 两种管理模式 8、校验方式：支持本地校验和网络校验 9、核心技术：核心内嵌，增强事件触发技术 10、部署模式：支持双机冗余部署 11、上传文件速度：≤5ms（50K 文件） 12、篡改检测时间：访问时实时检测 13、篡改恢复时间：≤6ms
篡改检测功能	通过在网页被访问时进行完整性检查杜绝网站向外发送被篡改的页面内容
	同时支持外挂轮询、核心内嵌及文件驱动过滤三种篡改检测技术
	支持网络检验
	提供水印签发工具，允许手工签发水印，并提供水印存储格式转换功能，允许其他格式的水印库导入到当前配置的水印库格式
	支持本地网页文件缓存和本地水印库缓存两种水印缓存形式
	可检测静态页面/动态脚本/多媒体文件；
	可以按不同容器选择待检测的网页；
	支持断线/连线状态下篡改检测；
	网页发送时比较网页和水印值；
	支持虚拟目录/虚拟主机；
	支持预先禁止非法程序对备份/保护目录的添加/删除/修改/更名/属性变更等操作；
支持对指定网页文件的恢复	
发布功能	支持与内容管理系统及各类发布工具的无缝集成；
	具备完善的发布同步功能，支持自动/手动精确同步，支持自动/手动增量同步；
	网页发布同时自动更新水印值；
	支持连线状态下网页恢复；
	同步和断线时都不影响检测；
	不影响原有的网页发布系统；

用途：WEB 应用安全（防篡改服务）	
指标项	指标（除特别说明外，以下为单台设备的配置）
	自动检测文件系统任何变化；
	文件变化自动同步到多个 Web 服务器；
	支持断线续传和失败重传，并支持从失败任务的日志文件导入任务
	发布服务器支持 Windows 和 Linux 操作系统平台
	支持自动恢复机制的启关
攻击防护功能	能够防护 SQL 数据库注入式攻击
	能够防护跨站脚本漏洞
	能够拦截敏感文件（*.dll、*.mdb 等）的访问；
	规则库采用正则表达式描述，规则扩展性高；
	允许自定义规则，全面支持网站防护能力的扩展；
报警功能	报警方式灵活：包括手机短信报警、邮件报警、声音报警等，并且可以跟用户本身的日志平台无缝集成；
	报警日志内容包括：日志记录时间戳、警报级别、服务器 ip、被篡改文件访问时间戳、被篡改文件路径、文件恢复状态等；
	具备完善的报警策略，支持报警级别、报警模式的自定义
	提供水印签发工具，允许手工签发水印，并提供水印存储格式转换功能，允许其他格式的水印库导入到当前配置的水印库格式
	支持本地网页文件缓存和本地水印库缓存两种水印缓存形式
	可检测静态页面/动态脚本/多媒体文件
	可以按不同容器选择待检测的网页
	支持断线/连线状态下篡改检测
	网页发送时比较网页和水印值

◆ 云服务市场安全服务

云服务市场安全服务可根据云服务平台用户使用需求进行及时补充，基于安全资源池物理硬件进行快速构建。各使用单位可根据自身单位安全需求在云服务市场进行自由选择。

云市场服务目录

虚拟防火墙	支持基于深度应用识别的访问控制、支持基于应用/角色的安全策略、支持静态路由、动态路由、策略路由、支持 NA；攻击防护：支持畸形报文攻击防护、支持多种 DoS/DDoS 攻击防护、支持 ARP 攻击防护；入侵防御：基于状态、精准的高性能攻击检测和防御、实时攻击源阻断、IP 屏蔽、攻击事件记录、支持针对 HTTP、SMTP、IMAP、POP3、VOIP、NETBIOS 等 20 余种协议和应用的攻击检测和防御。防火墙最大吞吐量：2Gbps；最大并发会话数:500K；每秒新建连接数:20K。
应用层防火墙	支持识别恶意请求含：跨站脚本 (XSS)、注入式攻击 (包括 SQL 注入、命令注入、Cookie 注入等)、跨站请求伪造等应用攻击行为；支持识别服务端响应内容导致的缺陷：敏感信息泄露、已有的网页后门、错误配置、目录浏览等缺陷；支持基于访问行为特征进行分析，能识别盗链、爬虫攻击的能力；支持识别网站中的网页木马程序,通过策略可防止木马网页被用户访问;支持 Cookie 防篡改、防劫持。
web 防篡改服务	篡改检测功能：通过在网页被访问时进行完整性检查杜绝网站向外发送被篡改的页面内容、支持外挂轮询、核心内嵌及文件驱动过滤三种篡改检测技术支持对指定网页文件的恢复；支持断线续传和失败重传，并支持从失败任务的日志文件导入任务、支持自动恢复机制；篡改检测时间：访问时实时检测；篡改恢复时间：≤6ms。
主机漏洞检测服务	检测漏洞数：大于 15000；检测配置检查项数：大于 2000；Web 扫描漏洞数：大于 1000；扫描 ip 限制：无限。
主机防病毒服务	支持智能识别蠕虫或者木马软件。采用智能型扫描机制，能够以文件真正格式作扫描。支持提供病毒隔离系统，将染毒文件安全隔离并备份。支持压缩文件查毒、清毒，压缩层次不少于 50 层，支持的压缩格式不少于 15 种。支持的加壳种类不少于 80 种。防（杀）病毒软件能够自动隔离感染而暂时无法修复的文件。邮件病毒检测及清除能力：采用宏指纹识别技术更有效的查杀 OFFICE 宏病毒。支持共享文件的病毒查杀。具有未知病毒检测、清除能力。

五、付款方式

付款方式：本项目的每笔款项均以人民币方式支付，支付的所需文件、时间和金额如下：

1. 合同；

2. 中标通知书；

3. 付款方式：合同签订之日 30 个工作日内招标人向中标人支付合同总价的 30%费用，项目验收完成后，招标人向中标人支付合同总价 70%，项目完成后 60 个工作日内结清。中标人需在招标人缴费的 7 个工作日内向招标人提出书面结算报告并出具发票；招标人以银行划帐方式支付中标人的服务经费。

第四章 合同

（《采购人需求》中另有规定的，以采购人需求为准）

注：本合同条款仅供参考，甲乙双方可根据实际情况进行补充。

技术服务合同书

甲方（委托方）：

乙方（受托方）：

依据《中华人民共和国合同法》的规定，合同双方就_____项目技术服务，经协商一致，签订本合同。

本合同根据项目采购文件（项目编号：_____）和该项目的中标（成交）通知书由甲方（委托方）与乙方（受托方）签订，并经双方协商同意下列条款：

第一条 下列文件均为本合同不可分割部分

1. 中标（成交）通知书；
2. 项目采购文件（项目编号：_____）；
3. 受托方中标（成交）的投标（报价）文件。
4. 在项目实施过程中双方共同签署的补充与修正文件。

各文件之间不一致的，以对受托方要求高的条款为准。

以上文件与合同附件具有同等法律效力，若以上文件与本合同有差异的，以本合同内容为准。

第二条 合同性质

本合同属于技术服务合同。

第三条 签约时间和地点

本合同由上述签约方于 201__ 年月日在市____区签订。

第四条 项目名称

项目。

第五条 服务内容

5.1 服务的要求和方式：

本项目的主要内容是受托方向委托方提供以下技术服务：

上述各项工作的具体内容以采购文件有关规定为准。如由于实际情况发生变化，委托方变更（包括修改、增删等）以上内容的，受托方同意无条件予以配合，且不另行向委托方收取任何费用；若导致受托方工作量或成本减少的，双方另行协商合同服务费用。

合同签订的同时，双方共同组成项目管理委员会，作为项目协调的最终决定机构，指定专门人员负责双方的协调事宜，并负责除合同本身之外的本项目其他确认事宜。委托方有权在书面通知受托方后更换专门人员。

5.2 技术服务质量保证：

。

第六条 计划安排

受托方提供服务的地点：委托方指定的。

受托方提供服务的期限：。

服务验收：受托方提出书面验收申请，委托人应组织验收，验收时间地点由委托人确定。服务质量验收合格的，委托人向受托方出具《项目验收报告》。

委托人在任何时候发现受托方服务不符合约定的，均可向受托方提出异议，受托人应予以改正并依本合同约定承担相应责任。

第七条 工作条件

委托方在正常工作时间内依申请向受托方提供资料、数据等，包括：。

第八条 技术服务人员条件

受托方必须承诺具有履行本合同的条件和资质，并保证按照委托方要求足够的技术人员和时间投入技术服务中，且在项目执行过程中项目负责人和主要工作人员未经委托方书面许可，不得变更。该项目的负责人负责与委托方的接洽工作。

第九条 保密要求

1. 受托人承诺，合同履行期间及终止后，受托方必须采取措施对本项目服务过程中的数据、技术文档等资料保密。由于受托方原因导致的上述资料泄密，受托方必须承担一切责任。合同终止后，受托方必须归还和删除本项目相关的所有数据和技术文档。

2. 受托方在此承认并同意，甲乙双方签署或进行的包括但不限于本合同、其他协议、文件、陈述或受托方因履行本合同所接触或知晓的委托方工作秘密（包括但不限于委托方的商业秘密、任何技术性资料、以及委托方为完成本合同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）均为本合同约定保密信息。

3. 受托方在此承诺并保证，受托方（包括但不限于受托方雇员、代理人、顾问等人员，下同）采取有效的保密措施以避免泄露给任何第三方；在本合同有效存续期间及合同终止后，未经委托方事先的书面同意，不得以任何方式公布、发表、公开、披露、散播、复制此种保密信息的任何部分，或对

其加以任何形式的利用或使用；如委托方要求，受托方必须签署委托方提供的保密协议。

4. 若受托方违反上述保密义务的，全部收益归委托方所有，受托方向委托方支付合同总金额的30%作为违约金，并另行应赔偿委托方因此遭受的全部损失（包括相应律师费用、差旅费等）。

5. 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“保密要求”条款均始终有效。

第十条 费用及支付方式

本合同费用总额为元（人民币整）。除前述款项外，受托方不得再向委托方收取其他费用，也不得要求委托方另行承担任何义务。

服务合同委托方费用，按如下支付方式支付：

受托方为委托方开具等额正式发票后委托方安排付款事宜，否则委托方有权拒绝付款，且不负任何责任。因财政拨款等非因委托方原因导致付款延迟或出现其他不符合前述约定的情形，委托方不承担任何责任。

受托方开户银行名称、地址和帐号为：

开户银行：

地 址：

帐 号：

委托方向上述账号汇出款项即视为委托方已履行付款义务，在合同履行过程中，因受托方账户的原因（包括但不限于账号被注销、被冻结等）导致受托方无法收取款项的，由受托方承担相应后果。

委托方应向受托方提供项目所需数据资料，因委托方过错导致项目延迟或停顿的，由委托方承担责任。

因受托方的原因造成项目延迟或停顿的，委托方有权终止合同。

第十二条 合同的变更

经签约方确认，在合同履行过程中对于具体内容需要变更的，由签约各方另行协商并书面约定，作为本合同的变更文本。

第十三条 违约责任与合同的解除

1. 受托方不履行合同或履行合同不符合约定或委托方的其他合理要求，委托方有权视具体情形扣除相应的服务费用，并有权要求受托方支付相当于该扣除部分服务费用30%的违约金；给委托方造成损失的，受托方应另行予以赔偿。

2. 受托方未按时完成本合同项下工作的（包括阶段工作成果及最终工作成果），每逾期一日，受托方同时应按合同总金额的1%向委托方支付违约金，并另行赔偿委托方损失。

3. 未经委托方书面同意，受托方任何时候均不得擅自中止或终止合同履行，否则，应按合同总金

额的 30%向委托方支付违约金，并另行赔偿委托方损失。

4. 有以下情形之一的，委托方有权解除合同，受托方需退还委托方已支付的所有款项，并按合同总金额的 30%向委托方支付违约金，且应另行赔偿委托方因此遭受的全部损失：

(1) 受托方未按时完成本合同项下工作，逾期超过[5]日的；

(2) 受托方发生累计两次或以上违约行为；

(3) 受托方履行义务不符合约定，经委托方提出后合理期限内仍未改正的；

(4) 未经委托方书面同意，受托方将本合同项下的权利或义务转让，或将本合同项下服务转包或分包的；

(5) 未经委托方书面同意，受托方将本合同项下成果作为己用或交付第三人使用的；

(6) 受托方在本合同有效期内丧失履行本合同的能力、经营范围和经营资质，或者因任何原因被注销、撤销、或吊销该证明受托方具备履行本合同能力、经营范围和经营资质的执照、证明或许可证书的。

5. 受托方违约行为存在多种责任约定的，委托方可自行选择主张方式（包括但不限于择一或同时主张）。

6. 本合同委托方损失包括但不限于委托方及相关方的实际损失、可得利益损失、委托方为处理违约事件所发生的包括调查费、评估费、公证费、仲裁费、诉讼费、律师费、交通费、差旅费等费用在内的费用和开支等；若受托方违约行为导致委托方遭受第三方的指控时，损失亦包括委托方为应诉等行为和承担其他不利义务而支付的一切费用。

7. 在合同履行过程中，因对方违约使合同不能继续履行或没有必要继续履行，签约方可在十日内通知对方解除合同。

8. 乙方在履行本合同过程中应接受甲方的监督与指导，若甲方提出修改意见的，乙方应及时予以修改直至符合甲方要求，否则甲方可根据具体进度将相关工作交由第三方完成，由此产生的费用和责任从乙方可取得的合同价款中扣除，具体金额由甲方根据具体影响情况决定。

9. 乙方指派服务人员应当具备完成本合同约定服务的能力、技能、资质和职业道德。乙方人员在履行本合同过程中遭受人身、财产损害或者造成他人人身、财产损害的，由乙方承担全部责任，给甲方造成损失的，乙方应当向甲方赔偿。

第十四条 争议解决方式

合同履行过程中如一方提议对合同做修改或补充，必须在所需更改的内容生效十日以前以书面方式提出，经对方同意并鉴定、补充合同书后进行。

合同履行过程中双方如有争议，应友好协商解决，协商不成，双方同意向合同签订地人民法院提出诉讼解决。

第十五条 其它

合同的生效：本合同自双方授权代表签字盖章之日起生效。

如遇不可抗力（不可抗力指双方在订立合同时不能预见、对其发生和后果不能避免且不能克服的事件，鉴于网络的特殊性质，不可抗力亦应包括但不限于黑客攻击、计算机病毒发作、国家政策法律变更和电信部门技术调整导致之影响、因政府管制而造成的暂时性关闭等在内的任何非甲乙双方人为因素影响网络正常经营之情形。），不可抗力导致本合同部分或全部无法继续履行的，受托人应自不可抗力事件发生之日起 20 日内出具不可抗力导致合同不能履行的证明，并采取适当措施减轻损失，双方互不负任何责任，并可协商是否终止本合同。

委托方在本合同履行过程中向受托方发出或者提供的所有通知、文件、文书、资料等，均以本合同所列明的地址送达。受托方如果迁址或者变更电话，应当书面通知委托方，未履行通知义务的，委托方按原地址邮寄相关材料即视为已履行送达义务。当面交付上述材料的，在交付之时视为送达；以邮寄方式交付的，寄出或者投邮后即视为送达。

本合同正本一式 份，甲方 份，乙方 份，采购代理机构一份。

（以下无正文）

甲方： 乙方：

（盖章）

（盖章）

法定代表人(或委托代理人)

法定代表人(委托代理人)

签字：

签字：

日期：

日期：

第五章磋商细则

一 说明

1. 概述

根据有关规定，遵循“公平、公正、科学、择优”的原则，结合本项目的技术和商务需求，由广州群生招标代理有限公司编制本磋商细则，并经磋商小组确认。内容包括本次竞争性磋商的过程和方法。

2. 磋商小组的组成

全部磋商过程由依法组建的磋商小组负责完成，磋商小组由三人单数专家组成。磋商小组下设工作小组，主要由采购代理机构工作人员组成，负责整理文件等工作。

二 磋商须知

1. 关于磋商方案

磋商小组应当严格遵守磋商纪律和磋商工作规则，按照磋商文件载明的磋商方法、评审标准开展磋商活动。

2. 关于磋商

(1) 采购代理机构负责主持整个磋商会议；

(2) 在磋商活动中，磋商小组应当根据《磋商文件》分别与每一位报价人进行单独磋商，并根据磋商小组将综合考虑货物技术性能指标、报价人综合实力、最终报价、服务期限、保修期、服务承诺及报价人提供的其他优惠条件等。使用综合评分法，推荐满足磋商文件全部实质性要求且按评审因素的量化指标评审得分最高的供应商为成交候选供应商，其余依次替补。

3. 关于纪律

(1) 磋商小组成员不得与任何报价人或者与磋商结果有利害关系的人进行私下接触，不得收受报价人、中介人、其他利害关系人的财物或者其他好处；

(2) 磋商小组成员应本着客观、公正的原则独立给出评价意见；

(3) 磋商小组成员之间不得相互串通进行评分；

(4) 磋商小组成员不得试图影响其他磋商小组成员的评价意见；

(5) 磋商小组应关闭通讯工具或设置为振动状态，并统一交由工作人员保管。

4. 关于回避

有下列情形之一的，不得担任磋商小组成员，如事先不知情的，应在采购代理机构宣读报价人名单及工作纪律后主动提出回避：

- (1) 参加采购活动前 3 年内与供应商存在劳动关系；
- (2) 参加采购活动前 3 年内担任供应商的董事、监事；
- (3) 参加采购活动前 3 年内是供应商的控股股东或者实际控制人；
- (4) 与供应商的法定代表人或者负责人有夫妻、直系血亲、三代以内旁系血亲或者近姻亲关系；
- (5) 与参加该采购项目供应商发生过法律纠纷的；
- (6) 磋商小组中，同一任职单位评审专家超过二名的；
- (7) 任职单位与采购人或参加该采购项目的供应商存在行政隶属关系的（不含采购人代表）；
- (8) 参与磋商文件论证的（不含采购人代表）；
- (9) 与供应商有其他可能影响采购活动公平、公正进行的关系；

5. 关于磋商小组成员责任

- (1) 磋商小组应在其书面意见上签字确认；
- (2) 磋商小组对其所提出的意见承担个人责任。

6. 关于保密

- (1) 磋商小组成员评审时，应各自独立进行评审，不得发表任何具有倾向性、诱导性或歧视性的见解，不得对其他评委的评审意见施加任何影响；
- (2) 磋商小组成员和与磋商活动有关的工作人员不得透露对报价文件的评审和比较、成交候选人的推荐情况以及磋商有关的其他情况；
- (3) 前款所称与磋商活动有关的工作人员，是指磋商小组成员以外的因参与磋商监督工作或者事务性工作而知悉有关磋商情况的所有人员。

三 磋商原则

磋商工作应依据有关规定，遵循“公平、公正、科学、择优”的原则进行。

四 磋商流程

1. 递交及接收报价文件

1.1 采购代理机构按《磋商文件》规定的时间和地点接收报价文件和组织磋商会。报价人必须派法定代表人或其授权代表人参加并签到；对于首次报价及最终报价，采购代理机构将公开唱出，由报价人

法定代表人或其授权代表人签名确认。采购代理机构负责做好有关记录。报价人不派出其授权代表参加开标会的，视为完全同意开标内容及对开标会过程无异议。

1.2 响应供应商授权代表必须持本人身份证原件参加磋商会，如响应供应商代表非法定代表人，还应持法定代表人授权委托书。

1.3 开封报价文件前，由响应供应商代表（按签到先后顺序的前三家响应供应商代表）检查磋商响应文件的密封情况，也可以由采购人委托的机构检查并见证，经确认无误后由响应供应商的授权代表抽签决定磋商顺序。

2、磋商说明

2.1 磋商小组应当对响应文件进行评审。进行初步评审时，磋商小组要审查每份响应文件是否符合《资格性及符合性审查表》的要求，同一品牌同一型号的产品可有多家响应供应商参与竞争，但只作为一个响应供应商计算，未实质性响应磋商文件的响应文件按无效响应处理，磋商小组应当告知提交响应文件的供应商。

磋商过程中出现下列情况之一时，本项目作废标处理：

1) 符合专业条件的供应商或者对报价文件作实质响应的供应商不足三家的；

（注：1、如果多个供应商所报产品全部是同一品牌同一型号的，只作为一个供应商计算。同一品牌不同型号的产品由多家供应商参加竞争，作为不同的供应商计算。2、采用竞争性磋商采购方式采购的服务项目，在采购过程中符合要求的供应商只有 2 家的，竞争性磋商采购活动可以继续。）

2) 报价人的报价均超过了采购预算，采购人不能支付的；

3) 因重大变故，采购任务取消的。

审查内容详见附表：资格性、符合性审(检)查表。

2.2 磋商小组在对响应文件的有效性、完整性和响应程度进行审查时，可以要求供应商对响应文件中含义不明确、同类问题表述不一致或者有明显文字和计算错误的内容等作出必要的澄清、说明或者更正。供应商的澄清、说明或者更正不得超出响应文件的范围或者改变响应文件的实质性内容。磋商小组将只对确定为实质上响应磋商文件要求的报价文件，即通过资格性、符合性审(检)查表的报价文件进行评价和比较。

2.3 对磋商文件中描述有歧意或前后不一致的地方，磋商小组有权进行评判，但对同一条款的评判应适用于每个响应供应商。

2.4 磋商小组要求供应商澄清、说明或者更正响应文件应当以书面形式作出。供应商的澄清、说明或者更正应当由法定代表人或其授权代表签字或者加盖公章。由授权代表签字的，应当附法定代表人授权书。供应商为自然人的，应当由本人签字并附身份证明。

2.5磋商小组所有成员应当集中与单一供应商分别进行磋商,并给予所有参加磋商的供应商平等的磋商机会,磋商内容形成磋商纪要文件。

2.6在磋商过程中,磋商小组可以根据磋商文件和磋商情况实质性变动采购需求中的技术、服务要求以及合同草案条款,但不得变动磋商文件中的其他内容。实质性变动的内容,须经磋商小组的一致同意,任何形式的决定须以符合公平、公正原则和有利于项目的顺利实施为前提。

2.7对磋商文件作出的实质性变动是磋商文件的有效组成部分,磋商小组应当及时以书面形式同时通知所有参加磋商的供应商。

2.8供应商应当按照磋商文件的变动情况和磋商小组的要求重新提交响应文件,并由其法定代表人或授权代表签字或者加盖公章。由授权代表签字的,应当附法定代表人授权书。供应商为自然人的,应当由本人签字并附身份证明。

2.9在磋商过程中,响应供应商提交的澄清、说明或者更正文件和最终报价文件,由响应供应商法人代表或授权代表签署后生效,响应供应商应受其约束。

2.10已提交响应文件的供应商,在提交最后报价之前,可以根据磋商情况退出磋商。采购代理机构应当退还退出磋商的供应商的磋商保证金。

2.11磋商结束后,磋商小组应当要求所有实质性响应的供应商在规定时间内提交最后报价及作出有关承诺。如磋商小组没有对磋商文件作实质性变动增加新的需求,第二次报价不得高于第一次报价。除非供应商另有说明,最终报价总价与第一次报价总价下浮的比例,其报价明细项按相同比例下浮。

2.12经磋商确定最终采购需求和提交最后报价的供应商后,由磋商小组采用综合评分法对提交最后报价的供应商的响应文件和最后报价进行综合评分。

2.13综合评分法,是指响应文件满足磋商文件全部实质性要求且按评审因素的量化指标评审得分最高的供应商为成交候选供应商的评审方法。磋商小组没有义务必须接受最低报价的报价人的报价。

3、评分及其统计

(1) 计算综合得分

评审时,磋商小组各成员应当独立对每个有效响应的文件进行评价、打分,然后汇总每个供应商每项评分因素的得分。磋商小组全部成员的服务或商务评分的算术平均值即为该响应供应商的服务或商务评分。然后,评出该响应供应商的价格评分。将各响应供应商的服务评分、商务评分和价格评分相加得出其综合得分。将各综合得分由高到低顺序排列,综合得分相同的,按下列顺序比较确定:(1) 评标价(由低到高);(2) 服务评分(由高到低)。如以上都相同的,名次由磋商小组抽签确定。磋商小组按上述排列向采购人推荐综合总得分第一名为成交候选供应商,其余依次为成交备选供应商。

(2) 分值(权重)分配

评分总分最高为100分，商务、服务及价格评分分值（权重）分配设置如下：

分值比例	商务评分	服务评分	价格评分
100	40	50	10

(3) 价格评审：

1) 价格分统一采用低价优先法计算，即满足磋商文件要求且最后报价最低的供应商的价格为磋商基准价，其价格分为满分。其他供应商的价格分统一按照下列公式计算：

$$\text{磋商报价得分} = (\text{磋商基准价} / \text{最后磋商报价}) \times \text{价格权值} \times 100$$

五 确定成交供应商

1、磋商小组应当根据综合评分情况，按照评审综合得分由高到低顺序推荐成交候选供应商，并编写评审报告。

2、采购代理机构应当在评审结束后2个工作日内将评审报告送采购人确认。

3、采购人应当在收到评审报告后5个工作日内，从评审报告提出的成交候选供应商中，按照排序由高到低的原则确定成交供应商，也可以书面授权磋商小组直接确定成交供应商。

4、采购人或者采购代理机构应当在成交供应商确定后2个工作日内，在指定信息发布媒体上公告成交结果，同时向成交供应商发出成交通知书。

5、替补候选人的设定与使用

排名第一的成交候选供应商放弃成交、或因不可抗力提出不能履行合同、或者竞争性磋商文件规定应当递交履约担保而在规定的期限内未能递交、或成交候选供应商拒绝与采购人签订合同的，采购人可以按照评审报告推荐的成交候选供应商名单排序确定下一候选供应商作为成交供应商，也可以重新开展采购活动。拒绝签订合同的成交供应商不得参加对该项目重新开展的采购活动。

6、磋商失败的情形：

出现下列情形之一的，采购人或者采购代理机构应当终止竞争性磋商采购活动，发布项目终止公告并说明原因，重新开展采购活动：

(1) 因情况变化，不再符合规定的竞争性磋商采购方式适用情形的；

(2) 出现影响采购公正的违法、违规行为的。

六 磋商评审附表

附表1：资格性及符合性审查表

评审内容	报价人名称		
具备磋商文件中规定报价人资格要求			
报价唯一，不高于采购人需求规定的最高限价或低于成本价报价且能提供相关证明材料的			
已按磋商文件规定提交报价保证金			
符合报价文件的签署、盖章要求			
报价人提供的资格证明材料齐全或者经磋商小组要求能在磋商小组规定的时间内补充齐全			
符合磋商文件报价有效期要求的			
满足磋商文件中带★号的条款和指标，且符合磋商文件的其他要求，没有重大偏离的			
未发现无效报价的其他情形的（见注1）			
最终的商务技术响应没有重大偏离或保留			
结论			

注：无效报价的其他情形

（1）评标期间，报价人没有按评标委员会的要求提交经授权代表签字的澄清、说明、补正或改变了报价文件的实质性内容的；

（2）经谈判小组认定报价文件提供虚假材料的；

（3）报价人以他人的名义报价、串通报价、以行贿手段谋取成交或者以其他弄虚作假方式报价的；

（4）报价人对采购人、采购代理机构、谈判小组及其工作人员施加影响，有碍采购公平、公正的；

（5）报价文件附有采购人不能接受的条件；

（6）出现不符合相关法律、法规要求的情况的。

1、报价人分栏中填写“○”表示该项符合磋商文件要求，“×”表示该项不符合磋商文件要求；

2、结论栏中填写“通过”表示该报价人报价文件符合磋商文件要求，“不通过”表示该报价人报价文件不符合文件要求；

3、结论汇总意见采取少数服从多数原则，即超过半数谈判小组成员的结论为“通过”则该报价人通过资格审查及符合性检查，否则不通过。

附表2：商务评审表（40分）

序号	评审项目	评审细则	分值 (40)
1	报价人拟派项目经理经验及资质能力水平情况	1、具有信息系统项目管理师（高级）资格证书； 2、具有 CISSP 证书（注册信息系统安全师）； 3、具有 PMP 项目管理资质证书； 4、具有网络规划设计师证书（高级）； 项目经理本人同时具备以上 4 个的得 6 分，具有 3 个的得 4 分，具有 2 个的得 2 分，具有 1 个的得 1 分，其他得 0 分。 注：须提供上述人员的证书，在本公司任职的外部证明材料（如加盖政府有关部门印章的打印日期在本项目投标截止日之前六个月内的《投保单》或《社会保险参保人员证明》，或单位代缴个人所得税税单等，否则无效。	6
2	报价人质量管理体系证明，提供证明文件复印件及国家认证认可监督管理委员会网上查询结果截图（分公司投标的，总公司资质可纳入评审）	提供有效的 ISO9001、ISO14001、ISO27001、OHSAS18001 认证证书，每个少一个扣 3 分，扣完为止。	9
3	报价人在项目所在地的稳定的技术服务人员情况	横向比较报价人在项目所在地稳定的技术服务人员数量：人数最多的，得 3 分；人数次之的，得 2 分；人数第三的，得 1 分；其他情况，不得分。 注：须提供上述人员的相关证书，在本公司任职的外部证明材料（如加盖地区政府有关部门印章的打印日期在本项目投标截止日之前六个月内的《投保单》或《社会保险参保人员证明》，或单位代缴个人所得税税单等。非本地公司在外地购买社保的必须提供技术服务人员在本地居住证（或暂住证）等在本地工作的证明文件）复印件。	3
4	项目主要技术管理人员情况	具有国家工信部（或原信息产业部）颁发的高级工程师职称，每人 1 分，满分 3 分。 具有国家工信部（或原信息产业部）颁发的中级工程师职称，每人 1 分，满分 3 分。 本项最分 6 分。 注：须提供上述人员的证书，在本公司任职的外部证明材料（如加盖地区政府有关部门印章的打印日期在本项目投标截止日之前六个月内的《投保单》或《社会保险参保人员证明》，或单位代缴个人所得税税单等。非本地公司在外地购买社保的必须提供技术服务人员在本地居住证（或暂住证）等在本地工作的证明文件）复印件。	6
5	本地综合服务支撑能力	报价人在项目实施地有服务机构的，得 3 分；没有的，得 0 分。	3

6	企业综合实力	<p>具有信息系统集成及服务一级资质，得4分；二级资质，得2分，其他情况不得分。</p> <p>具有CMMI5证书，得4分；CMMI3证书，得2分，其他情况不得分。</p> <p>具有信息安全等级保护测评机构推荐证书，得2分；否则不得分。</p> <p>注：提供证书复印件并加盖投标人公章为准。</p>	10
7	其他信誉（守合同重信用证明）	有，得1分；其他情况，0分。	2
8	对不良信用记录的扣分	<p>以“信用中国”（www.creditchina.gov.cn）网站为查询渠道，对列入企业经营异常名录的供应商每一条记录扣0.1分，最高扣1分；未列入则不扣分（如查询结果显示“没查到您要的信息”，视为未列入企业经营异常名录）。评审时评标委员会应将信用信息查询记录和证据截图存档。</p>	1

备注：报价人应提交与评价指标体系相关的各类有效资料，复印件加盖公章。

附表2：服务评审表（50分）

序号	评审内容	评分细则	分值（50）
1	对项目背景、现状及总体需求的理解情况	根据报价人提供的材料进行横向对比，对比最优，得4分；对比次之，得2分；对比一般，得1分；对比较差，得0分。	4
2	政务云机房服务能力	报价人需要提供不同地理位置的政务云机房的证明材料，3个或以上，得4分；2个，得2分；1个，得1分；其他，0分。	4
3	报价人自营的云平台稳定性、技术成熟性	根据报价人提供的材料进行横向评比各报价人自营云平台的产品成熟度、品牌社会接受程度。 1、产品近两年 IDC 针对国内软件定义计算市场占有率报告中排名前三的，第一名得5分，第二名得3分，第三名得1分，其它不得分。 2、品牌以业界主流云平台厂商为优，以 Gartner X86 服务器虚拟化魔力四象限推荐厂家报告为佐证，具有报告得2分，其它不得分。 3、比较云平台的架构的产品选型和技术架构设计能力，提供云平台虚拟化软件 1000CPU 以上的案例，须提供证明文件为佐证，提供案例 5 个或以上得3分，少于 5 个且不少于 3 个得2分，少于 3 个且不少于 1 个得1分，其它不得分。	10
4	政务云平台运营服务质量	对报价人政务云平台运营服务质量的评比考核对比，提供上一期的市信息化中心服务评分佐证。优，得6分；对比次之，得3分；对比一般，得1分；对比较差，得0分。	6
5	报价人运维经验	根据报价人提供的材料进行横向对比，比较政务云运维的经验，须提供合同等有效的佐证材料，经验3年或以上得5分，少于3年且不少于1年得2分，其它不得分。	5
6	政务云部署能力	报价人需要提供成功案例（需要提供证明材料）。3个或以上，得6分；2个，得4分；1个，得2分；其他，0分。	6
7	业务上云的迁移能力	报价人需提供网站开发商对上云迁移的方案可行性的确认函，有得5分，其他不得分。	5
8	项目实施方案	根据报价人提供的材料进行横向对比，对比最优，得4分；对比次之，得2分；对比一般，得1分；对比较差，得0分。	4
9	安全服务方案（考察报价人安全服务方案的完整性、合理性、可操作性）	根据报价人提供的材料进行横向对比，对比最优，得3分；对比次之，得2分；对比一般，得1分；对比较差，得0分。	3
10	培训及服务质量保证（针对服务进度保障情况、服务人员管理要求情况进行评估）。	根据报价人提供的材料进行横向对比，对比最优，得3分；对比次之，得2分；对比一般，得1分；对比较差，得0分。	3

备注：报价人应提交与评价指标体系相关的各类有效资料，复印件加盖公章。

第六章 报价文件格式

一、报价文件目录表

序号	文件名称	是否提交	页码范围	备注
一	初审文件			
1	★报价函（格式1）			
2	★报价一览表（格式2）			
3	★分项报价表（格式3）			
二	资格性、符合性审查文件			
4	★营业执照副本或事业单位法人证书副本（复印件，加盖公章）			
5	★法定代表人证明及授权书（格式4）			
6	★实质性条款响应一览表（格式5）			
7	★关于资格证明文件的声明函（格式6）			
8	其他资格证明文件			
三	商务、技术文件			
9	2017-2018年度财务报表及审计报告（复印件，加盖公章）			
10	商务技术评审自查表（格式7）			
11	2015年至今同类项目业绩表（格式8）			
12	报价人为本项目配置人员说明（格式自拟）			
13	质量保证、售后服务说明（格式自拟）			
14	与采购人需求差异表（格式9）			
15	合同条款响应一览表（格式10）			
16	缴交采购代理服务费承诺书（格式11）			
17	保证金汇款声明函（格式12）			
18	同意磋商文件条款说明（格式13）			
19	所报货物详细的技术方案（格式自拟）			
20	报价人认为需提交的其他资料			

二、报价信封

序号	文件名称	是否提交	备注
1	报价一览表（与报价文件中的内容保持一致）；		
2	分项报价表（与报价文件中的内容保持一致）；		
3	报价保证金汇款声明函（含保证金进账单复印件）		

- (1) 带“★”文件为必须提供的文件；
- (2) 上述文件如为复印件的，必须加盖报价人公章；
- (3) 报价人应自行承担所提供上述资料任何错漏而导致的一切后果。

格式 1 报 价 函

广州群生招标代理有限公司：

我方确认收到你方提供的_____项目及其相关服务的磋商文件的全部内容。我方：(报价人名称)作为报价者正式授权(授权代表全名、职务)代表我方进行有关报价的一切事宜。在此提交的报价文件，正本一份，副本两份。我方已完全明白磋商文件的所有条款要求，并重申以下几点：

1. 我方决定参加：项目编号为的报价；
2. 本报价文件的有效期为报价截止日后 90 天有效，如被确定为成交供应商，有效期将延至合同终止日为止；
3. 我方已详细研究了磋商文件的所有内容包括修正（如果有）和所有已提供的参考资料以及有关格式并完全明白，我方放弃在此方面提出含糊意见或误解的一切权利；
4. 我方同意按照你方可能提出的要求提供与报价有关的任何其它数据或信息；
5. 我方理解磋商小组不一定接受最低报价或任何你方可能收到的报价；
6. 我方如被确定为成交供应商，将保证履行磋商文件以及磋商文件修改书（如有的话）中的全部责任和义务，按质、按量、按期完成《合同》中的全部任务；
7. 我方自行完全承担因报价文件错误、缺漏、不清晰而导致的一切后果；
8. 我方确认此次磋商中提供的一切资料均是真实的，准确的，并完全承担因此产生的一切后果。
9. 我方的报价被接受，我方同意按照磋商文件规定向采购代理机构缴纳采购代理服务费用。

所有与本磋商文件有关的函件请发往下列地址：

报价人全称（加盖公章）：

地址： 邮政编码：

法定代表或其授权代表（签字）：

日 期： 年 月 日

格式 2 首次报价一览表

项目名称：

项目编号：

报价人名称	总报价 (人民币 元)	服务时间

注：1. 报价包括了项目的全部费用。

2. 本表格须附在正副本的报价文件中，并另封装一份在“报价信封”内，封口加盖公章。

报价人全称（加盖公章）：

法定代表或其授权代表（签字）：

日 期： 年 月 日

格式3 分项报价表

本表将有可能在成交公告中公开，请报价人仔细填写

项目名称：

项目编号：

序号	报价内容	单价	总价	备注
1				
2				
3				
...				
合计				

注：报价人须针对项目实际情况编制完整详细的项目报价。本表格须附在正副本的报价文件中，并另封装一份在“报价信封”内。

报价人全称（加盖公章）：

法定代表或其授权代表（签字）：

日期： 年 月 日

格式4 法定代表人证明及授权书

致：广州群生招标代理有限公司

本授权证明：（法定代表人姓名）是注册于（省、市、县）的（报价人名称）的法定代表人，现任（法定代表人职务）。在此授权（被授权人姓名、职务）作为我公司的全权代理人，在（项目名称）的报价（项目编号为：）及其合同执行过程中，以我公司的名义处理一切与之有关的事务。

本授权书于年月日签字生效，特此声明。

法定代表人

居民身份证正反面复印件粘贴处

被授权人(报价人授权代表)

居民身份证正反面复印件粘贴处

报价人全称（加盖公章）：

地址：

法定代表人（签字或签章）：

被授权人(报价人授权代表)（签字）：

格式 5

实质性条款响应一览表

项目名称：

项目编号：

序号	带“★”号响应内容	是否响应	偏离说明	响应页码
1	合格报价人资格要求			
2	报价文件格式带“★”内容			
3				
...				

说明：1、报价人必须对应磋商文件的“★”号条款逐条应答并按要求填写下表。

2、对完全响应的条目在下表相应列中标注“○”。对有偏离的条目在下表相应列中标注“×”，并简述偏离内容。

3、本表“是否响应”、“偏离说明”、“响应页码”不填写内容的视为完全响应。

格式 6

关于资格证明文件的声明函

广州群生招标代理有限公司：

我方愿响应你方年月日发布的_____项目（项目编号：）报价邀请，参与报价，提供采购人需求中规定的全部内容，并按磋商文件要求提交所附资格文件且声明和保证如下：

1. 我方为本次报价所提交的所有证明我方提供货物和服务合格和我方资格的文件是真实的和正确的，并愿为其真实性和正确性承担法律责任；核验我方提供相关复印件与原件不一致的，或我方无法在规定时间内提供原件的，采购人或采购代理机构有权取消我方报价或成交资格；提供给采购人的货物及服务与报价承诺一致。
2. 我方在参与本次报价时，符合报价人资格条件要求及其他法律法规规定要求。
3. 我方在参加本次报价近三年内，在经营活动及参与招标投标活动中没有重大违法活动及涉嫌违规行为，并没有因而被有关部门警告或处分的记录。
4. 我方如中标，除不可抗力原因外，将在规定时间内与采购人签订合同。

如有违反上述声明之情形，采购人有权取消我方中标资格并提交相关监管部门处理。

报价人全称（加盖公章）：

法定代表人或其报价人授权代表(签字)：

日 期： 年 月 日

格式7 商务技术评审自查表

序号	评审分项	内容	证明文件(如有)
1			见响应文件()页
2			见响应文件()页
3			见响应文件()页
4			见响应文件()页
5			见响应文件()页
...			

格式8 2015年至今同类项目业绩表

项目名称：

项目编号：

序号	业主名称	项目名称	合同总价	完成时间	业主单位 联系人及电话
1					
2					
...					
小计					

注：报价人应提供相关证明附件。

报价人全称（加盖公章）：

法定代表或其授权代表（签字）：

日期： 年 月 日

格式9 与采购人需求差异表

项目名称：

项目编号：

序号	磋商文件要求		报价文件内容	
	原条目	简要内容	是否响应	偏离说明
	一		
	二		
	三		

注：报价人应根据其提供的货物和服务，逐条对照磋商文件《采购人需求》的内容要求填写，有差异的，不论是技术或商务上，均须在此表中列明两者的简要内容，以便查对和评审。除“偏离说明”栏所列的内容外，其余按《采购人需求》的内容执行。本表提供空表的视为完全响应。

报价人全称（加盖公章）：

法定代表或其授权代表（签字）：

日期： 年 月 日

格式 10

合同条款响应一览表

项目名称：

项目编号：

序号	磋商文件合同要求	报价文件内容	
	条款号	是否响应	差异说明

注：1. 报价人应对照磋商文件第四章合同条款所列内容逐条对应填写，完全满足的在“是否响应”栏中填“响应”；有差异的则在“差异说明”栏中列出差异的具体内容。本表提供空表的视为完全响应。

2. 除“差异说明”栏所列的内容以外，其余按《合同书》格式中的条款执行。

报价人全称（加盖公章）：

法定代表或其授权代表（签字）：

日期： 年 月 日

格式 11

缴交采购代理服务费用承诺书

致：广州群生招标代理有限公司

如果我方在贵公司组织的项目名称：（项目编号：）磋商采购项目中被确定为成交供应商候选人，我方保证在收到《成交通知书》前，按照磋商文件的规定向贵公司交纳采购代理服务费。

我方如违约，愿凭贵公司开出的违约通知，按上述承诺金额的 200% 在采购人与我方签订的采购合同款项中扣付，并在此同意和要求采购人（应广州群生招标代理有限公司的要求）办理支付手续。

特此承诺！

报价人全称（加盖公章）：

法定代表或其授权代表（签字）：

日期： 年 月 日

格式 12**保证金汇款声明函**

致：广州群生招标代理有限公司

我方为项目（项目编号：）递交保证金人民币元（大写：人民币元）已于年月日以银行主动划账方式划入你方账户。

详见附件：银行出具的汇款单或转账凭证复印件。

退还保证金时请按以下内容划入我方账户。若因内容不全、错误、字迹潦草模糊导致该项目保证金未能及时退还或退还过程中发生错误，我方将自行承担全部责任和损失。

收 款 人	收款人名称			
	收款人地址			
	开户银行 (含汇入地点)		联系人	
	帐 号		联系电话	

报价人全称（加盖公章）：

地 址：

注：报价人应详细填写本文件，并按要求粘贴凭证复印件。银行进账单复印件（加盖公章）及保证金汇款声明应装在单独的“报价信封”内。

格式 13**同意磋商文件条款说明**

致：广州群生招标代理有限公司

为响应你方组织的项目名称：项目的竞争性磋商【项目编号：】，我方在参与报价前已详细研究了磋商文件的所有内容，包括修改文件（如果有的话）和所有已提供的参考资料以及有关附件，我方完全明白并认为此磋商文件没有倾向性，也没有存在排斥潜在报价人的内容，我方并同意磋商文件的相关条款。

特此声明。

报价人全称（加盖公章）：

法定代表或其授权代表（签字）：

日 期： 年 月 日