

衢州市政务云服务项目

招标文件

项目名称：衢州市政务云服务项目

项目编号：Qzkc2024-025

采购人：衢州市数字产业发展有限公司

采购代理机构：衢州市开成工程造价咨询事务所有限公司

二〇二四年八月

目 录

第一章 招标公告	3
第二章 投标人须知前附表及投标人须知	6
第三章 采购内容及要求	23
第四章 合同主要条款	28
第五章 评标办法	36
第六章 应提交的有关格式范例	39

第一章 招标公告

根据《衢州市国资委关于印发衢州市国有企业采购管理办法（试行）的通知》（衢国资发〔2020〕36号）等有关规定，衢州市开成工程造价咨询事务所有限公司受衢州市数字产业发展有限公司委托，就衢州市政务云服务项目进行公开招标，欢迎国内合格的投标人前来投标。

一、项目编号：Qzkc2024-025

二、项目名称：衢州市政务云服务项目

三、采购方式：公开招标

四、招标内容及要求：

序号	采购内容	数量/单位	采购预算价	最高限价
1	衢州市政务云服务项目	1项	19100万元	19100万元

五、合同履行期限：36个月（自采购人组织服务能力验证通过后起计，最迟不晚于2024年12月31日）。

六、投标人资格要求：

1. 符合《衢州市国有企业采购管理办法（试行）》第十五条规定：

(1)具有独立承担民事责任的能力；

(2)具有良好的商业信誉和健全的财务会计制度；

(3)具有履行合同所必需的设备、技术和售后保障等能力；

(4)有依法缴纳税收和社会保障资金的良好记录；

(5)参加采购、招投标等活动前3年内，在经营活动中没有重大违法记录和行贿犯罪记录；

(6)具有法律法规和规范性文件规定的其他条件。

2. 且必须为未被列入“信用中国”网站（www.creditchina.gov.cn）、中国政府采购网（www.ccgp.gov.cn）渠道信用记录失信被执行人、重大税收违法案件当事人名单、政府采购严重违法失信行为记录名单的投标人。

3. 单位负责人为同一人或者存在直接控股、管理关系的不同供应商，不得参加同一合同项下的采购活动。

4. 投标人自投标截止时间前三年内无行贿犯罪记录（以中国裁判文书网（网址：<http://wenshu.court.gov.cn/>）查询到的行贿判决书为准）。

5. 本项目接受联合体投标。

七、采购文件获取

1. 供应商按下述要求获取采购文件，如未在“衢州市阳光交易服务平台”系统内完成相关流程，引起投标无效，责任自负。

2. 本项目采购文件实行“衢州市阳光交易服务平台”在线申请获取采购文件，不提供纸质版采购文件。供应商获取采购文件前应先办理“衢州市阳光交易服务平台”供应商信息入库备案同时办理介质 CA 锁。完成介质 CA 锁办理预计 2~3 个工作日，建议各供应商合理安排办理时间。

3. 潜在供应商登录衢州市阳光交易服务平台 (<https://qzygjy.com/>) 办理供应商信息入库备案事宜，注册公示 24 小时无异议后入库。

4. 未办理企业信息入库的供应商，根据显示界面提示免费注册，填写、上传相关主体信息，带“*”号的必填，填好后“提交”。供应商须提前申领介质 CA 锁及电子签章，具体操作可参考衢州市阳光交易服务平台交易乙方操作手册。

5. CA 办理：

天谷 CA：<http://www.tseal.cn/tcloud/common.xhtml?projId=307> 天谷联系电话：400-087-8198。

6. 采购文件下载：

(1) 潜在供应商登录“衢州市阳光交易服务平台”，在线申请获取采购文件（选择采购公告，进入项目，选择“交易前阶段”进入项目在获取采购文件菜单中选择项目，选择“交易文件下载”）。

(2) 投标文件的解密：供应商按照平台提示和采购文件的规定在 30 分钟内于衢州市阳光交易服务平台不见面开标大厅完成在线解密。

7. 具体操作指南：详见衢州市阳光交易服务平台“办事指南—衢州市阳光交易服务平台供应商操作手册”，如遇平台技术问题详询 4009980000。

8. 投标工具

投标文件制作软件（衢州产交版），下载地址：<https://download.bqpoint.com/download/downloaddetail.html?SourceFrom=Ztb&ZtbSoftXiaQuCode=112601&ZtbSoftType=tballeinclusive> 联系方式，新点软件客服电话：4009980000/0570-3878007。

八、提交投标文件截止时间、开标时间和地点

1. 投标文件递交截止时间（开标时间，下同）：2024 年 8 月 30 日 09 时 00 分 00 秒。

2. 投标文件递交方式：电子投标文件采用网上递交的方式，上传至衢州市阳光交易服务平台（<https://qzygjy.com/TPBidder/memberLogin?type=13>）。

3. 网上开标地点：衢州市阳光交易服务平台不见面开标大厅（网址：<https://qzygjy.com/BidOpening/bidopeninghallaction/hall/login>）。操作手册见官网首页下载中心。

九、公告期限

自本公告发布之日起 5 个工作日。

十、其他补充事宜

供应商认为采购文件使自己的权益受到损害的，可以自获取采购文件之日或者采购文件公告期限届满之日（公告期限届满后获取采购文件的，以公告期限届满之日为准）起 7 个工作日内，以书面形式向采购人和采购代理机构提出质疑。质疑供应商对采购人、采购代理机构的答复不满意或者采购人、采购代理机构未在规定的时间内作出答复的，可以在答复期满后十五个工作日内向采购人监督管理部门投诉。

十一、对本次招标提出询问，请按以下方式联系。

1. 采购人名称：衢州市数字产业发展有限公司

联系人：赵先生 联系方式：15857073722

地址：衢州市柯城区白云街道三江东路 12 号 1 幢

2. 采购代理机构名称：衢州市开成工程造价咨询事务所有限公司

联系人：吕先生 联系方式：15305707858

地址：衢州市柯城区弈谷文体城二期 3-1

3. 监督部门名称：衢州市城市投资发展集团有限公司纪委

联系人：赵女士 联系方式：0570-8033001

衢州市数字产业发展有限公司

衢州市开成工程造价咨询事务所有限公司

2024 年 08 月 09 日

第二章 投标人须知前附表及投标人须知

一、投标人须知前附表

序号	内 容	说明与要求
1	项目名称	衢州市政务云服务项目
2	最高限价	19100 万元
3	投标有效期	自投标截止之日起 90 日历天。
4	现场踏勘	采购人不组织统一踏勘，投标人可自行踏勘。
5	是否采用电子招标投标	是，本项目实行不见面电子招投标方式。
6	投标文件份数	加密电子投标文件一份，包括“资格审查文件”“技术商务文件”“报价文件”三个部分组成，按规定上传至衢州市阳光交易服务平台。中标人在中标结果公告结束后，按采购人或代理机构要求提供与投标时一致的投标文件。
7	投标文件的签章	电子签章
8	投标文件递交截止时间及地点	将由投标文件制作工具制作生成的加密投标文件在投标截止时间前（以上传完成时间为准）上传至衢州市阳光交易服务平台（网址： https://qzygjy.com/ ）。
9	开标时间	2024 年 8 月 30 日 09 时 00 分 00 秒（北京时间）
10	样品	<p>1. 本项目是否需要样品：<input checked="" type="checkbox"/>否；<input type="checkbox"/>是，详见“第三章 采购内容及要求”；</p> <p>2. 样品标识：<input type="checkbox"/>明标，<input checked="" type="checkbox"/>暗标；</p> <p>3. 样品送至地点：衢州市柯城区芹江东路 288 号衢时代创新大厦 3 号楼负一楼西侧（衢州市产权交易中心有限公司）样品存放点；</p> <p>4. 样品递交截止时间：同开标时间；</p> <p>5. 中标人样品处理：<input type="checkbox"/>退还，<input type="checkbox"/>封存至验收，<input type="checkbox"/>抵扣采购数量；</p> <p>6. 其他要求：评标结束后 1 个工作日内，未中标供应商将其样品取回，逾期未取回的样品由采购人自行处理；中标供应商样品封存，作验收依据。</p>
11	现场演示	<p>1. 本项目是否需要现场演示：<input type="checkbox"/>否，<input checked="" type="checkbox"/>是；</p> <p>▲2、演示介绍视频存储在 U 盘介质密封在信封内（信封封口处须加盖单位公章）提供给招标代理公司（联系人：吕锋；联系电话 15305707858），要求在 2024 年 8 月 29 日 17：30 分前自行送往衢州市弈谷文体城二期 3-1 二楼，为避免不必要的麻烦，视频 U 盘不接收邮寄形式递交，逾期或以邮寄形式递交或未密封加盖公章的均不予接受，因此造成的后果，由投标人自行承担，不提供不得分。</p>

12	开标地点及平台	地点：衢州市柯城区芹江东路 288 号衢时代创新大厦 3 号楼负一楼西侧（衢州市产权交易中心有限公司）的开标厅。 开标平台：衢州市阳光交易服务平台不见面开标大厅（ https://qzygjy.com/BidOpening/bidopeninghallaction/hall/login ）。
13	投标文件开启程序	(1)投标文件开启时间到后，代理机构（或公证人员）宣布开始解密，30 分钟内供应商应完成投标文件的解密。供应商解密方式：供应商自行登录衢州市阳光交易服务平台不见面开标大厅（ https://qzygjy.com/BidOpening/bidopeninghallaction/hall/login ）——投标人身份——我的项目——选择标段——待代理开启解密后进行解密操作供应商在规定的时间内都已完成解密，则系统自动结束解密；供应商因自身原因未在规定时间内完成解密，则默认自动放弃； (2)采购代理机构导入投标文件成功后进入评标流程。
14	中标结果公告期限	1 个工作日
15	中标人履约保证金缴纳	合同签订前，中标人向采购人交纳中标价 1%的履约保证金（以现金、电汇或保函的形式）。电汇形式的服务期满后，中标人无任何违约、赔偿等情况的，采购人在 30 日内将履约保证金原额无息退还给中标人。以保函形式提供的，保函有效期应在合同期限上不少于 6 个月且保函到期时合同未履行完毕的，中标人应在保函到期前完成续保。
16	签订合同	发出中标通知书之日起 30 天内。
17	合同备案	中标人与采购人签订合同后，2 个日历天内将合同扫描件电子版发送至邮箱：353291769@qq.com；本项目采购合同按规定在衢州市阳光交易服务平台（网址： https://qzygjy.com/ ）予以备案。
18	采购公告、更正公告、中标结果公告发布网址	衢州市阳光交易服务平台（ https://qzygjy.com/ ）
19	其他注意事项	(1)采购文件中部分加“▲”的条款，属于采购文件的实质性要求和条件，着重提醒各投标人注意，并认真查看采购文件中的每一个条款及要求，因误读采购文件而造成的后果，采购人概不负责； (2)本项目实行不见面电子招投标方式，投标截止时间后投标人凭 CA 数字证书完成投标解密等事宜。投标人的联系电话在投标当天保持通信畅通，因通信问题无法联系到投标人造成的后果由投标人自行承担。
20	投标人信用查询	(1)采购代理机构将对本项目投标供应商的信用信息进行查询和甄别，查询渠道为信用中国网站（ www.creditchina.gov.cn ）、中国政府采购网（ www.ccgp.gov.cn ）； (2)截止时点：提交投标文件（响应文件）截止时间前 3 年内；

		<p>(3)信用信息查询记录和证据以网页截图方式留存；</p> <p>(4)不良信用记录指：</p> <p>①被列入信用中国网站“失信被执行人”“重大税收违法案件当事人名单”；</p> <p>②被列入中国政府采购网政府采购严重违法失信行为记录名单；</p> <p>(5)信用信息的使用规则：供应商存在不良信用记录的，其投标文件将被拒绝；</p> <p>(6)如允许联合体投标的，联合体成员存在不良信用记录视同联合体存在不良信用记录。</p>																										
21	开标特别说明	<p>(1)开标解密使用供应商上传的电子投标文件；</p> <p>(2)因供应商原因（包括供应商自主选择的CA证书、电脑环境、网络等），造成其电子投标文件未解密的，或投标文件解密了，但投标文件无法识别、读取的，视为撤销其投标文件；</p> <p>(3)供应商必须使用生成电子投标文件的CA数字证书解密电子投标文件。</p>																										
22	解释	本采购文件的解释权属于采购人和采购代理机构所有。																										
23	交易费用	<p>1、代理费、评委费、公证费、询价费按实计取，由中标人支付。</p> <p>2、进场交易场地费按实收取，由招标人与中标人按进场交易费用收费标准支付，进场交易费用收费标准按下表执行。</p> <p>账户名称：衢州市产权交易中心有限公司</p> <p>账户号码：1209210009049028267</p> <p>开户银行：中国工商银行股份有限公司衢州南湖支行</p> <table border="1" data-bbox="582 1294 1396 1971"> <thead> <tr> <th>中标价</th> <th>分档收费标准</th> <th>备注</th> </tr> </thead> <tbody> <tr> <td>100万（含）以下</td> <td>1000元</td> <td>1、费用由中标单位承担。</td> </tr> <tr> <td>100万-200万（含）</td> <td>1600元</td> <td rowspan="2">2、项目废标后再次进场交易的由最终的中标单位承担，</td> </tr> <tr> <td>200万-500万（含）</td> <td>4000元</td> </tr> <tr> <td>500万-1000万（含）</td> <td>12000元</td> <td rowspan="2">废标后不再进场交易的项目由采购单位按照第二档100万-200万（含）的收费标准承担50%（即：800元）；</td> </tr> <tr> <td>1000万-2000万（含）</td> <td>20000元</td> </tr> <tr> <td>2000万-5000万（含）</td> <td>30000元</td> <td rowspan="3">3.无法确定交易（中标）金额的项目，按照第二档100万-200万（含）的收费标准执行。</td> </tr> <tr> <td>5000万-1亿（含）</td> <td>40000元</td> </tr> <tr> <td>1亿-5亿（含）</td> <td>60000元</td> </tr> <tr> <td>5亿-10亿（含）</td> <td>80000元</td> <td></td> </tr> </tbody> </table>	中标价	分档收费标准	备注	100万（含）以下	1000元	1、费用由中标单位承担。	100万-200万（含）	1600元	2、项目废标后再次进场交易的由最终的中标单位承担，	200万-500万（含）	4000元	500万-1000万（含）	12000元	废标后不再进场交易的项目由采购单位按照第二档100万-200万（含）的收费标准承担50%（即：800元）；	1000万-2000万（含）	20000元	2000万-5000万（含）	30000元	3.无法确定交易（中标）金额的项目，按照第二档100万-200万（含）的收费标准执行。	5000万-1亿（含）	40000元	1亿-5亿（含）	60000元	5亿-10亿（含）	80000元	
中标价	分档收费标准	备注																										
100万（含）以下	1000元	1、费用由中标单位承担。																										
100万-200万（含）	1600元	2、项目废标后再次进场交易的由最终的中标单位承担，																										
200万-500万（含）	4000元																											
500万-1000万（含）	12000元	废标后不再进场交易的项目由采购单位按照第二档100万-200万（含）的收费标准承担50%（即：800元）；																										
1000万-2000万（含）	20000元																											
2000万-5000万（含）	30000元	3.无法确定交易（中标）金额的项目，按照第二档100万-200万（含）的收费标准执行。																										
5000万-1亿（含）	40000元																											
1亿-5亿（含）	60000元																											
5亿-10亿（含）	80000元																											

二、投标人须知

(一) 总则

1. 适用范围

本采购文件适用于本次采购活动中所叙述的衢州市政务云服务项目。

2. 定义解释

- (1) “采购人”是指衢州市数字产业发展有限公司；
- (2) “采购代理机构”是指衢州市开成工程造价咨询事务所有限公司；
- (3) “项目”系指投标人按采购文件规定向采购人提供的货物或服务；
- (4) “投标人”是指获得采购文件并向采购代理机构提交投标文件的供应商；
- (5) “潜在投标人”是指符合本采购文件中投标人资格要求的合格供应商；
- (6) “中标人”是指经评审小组审查通过，并经公告无异议的投标人；
- (7) “投标人代表”是指投标人法定代表人或被投标人法定代表人授权委托的人；
- (8) “货物”系指投标人按采购文件规定向采购人提供的各类设备、软件、产品、技术资料及使用手册等；
- (9) “服务”系指本项目采购内容本身及相关的售后技术支持、培训服务等相关服务；
- (10) “▲”系指按本采购文件要求投标人必须实质性响应的条款，有任何一项缺失或非实质性响应将取消其投标资格。

3. 项目说明

(1)本采购项目说明详见采购文件投标须知前附表；

(2)本采购项目根据《衢州市国资委关于印发衢州市国有企业采购管理办法（试行）的通知》（衢国资发〔2020〕36号）等有关法律、行政法规和部门规章，通过公开招标方式选定中标人。

4. 采购方式

公开招标

5. 合格投标人的条件

凡符合本采购文件第一章招标公告投标人资格要求的均为合格的投标人。

6. 投标费用

无论招投标过程中的做法和结果如何，投标人自行承担招投标活动中所发生的全部费用。

7. 知识产权

(1)投标人应保证在本项目使用的任何产品和服务（包括部分使用），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法律或经济纠纷。如因专利权、商标权或其它知识产权原因引起法律或经济纠纷的，所有相关责任由投标人承担；

(2)采购人享有本项目实施过程中产生的知识成果及知识产权；

(3)如采用投标人所不拥有的知识产权，则在投标报价中必须包括投标人合法获得该知识产权的相关费用，无论投标人是否在投标报价中单独列明，采购人均视为投标报价已包含该部分费用。

8. 转包或分包

(1)本项目不允许转包或分包；

(2)经采购人同意后允许分包。

9. 其他

(1)如发现采购文件及其评标办法中存在含糊不清、相互矛盾、多种含义以及歧视性不公正条款或违法违规等内容时，请在规定的询疑时间前同时向采购人、采购代理机构书面反映，逾期不得再对采购文件的条款提出质疑；

(2)本采购文件及相应的补充文件、通知等解释权归采购人和采购代理机构所有。

10. 特别说明

(1)▲多家投标人参加投标，单位负责人为同一人或者存在直接控股、管理关系的不同投标人，不得参加同一合同项下的采购活动；

(2)提供相同品牌产品且通过资格审查、符合性审查的不同投标人参加同一合同项下投标的，按一家投标人计算，评审后得分最高的同品牌投标人获得中标人推荐资格；评审得分相同时，以报价低者获得中标人推荐资格；

(3)非单一产品采购项目中，多家投标人提供的核心产品品牌相同的，按一家投标人认定；

(4)▲投标人投标所使用的资格、信誉、荣誉、业绩与企业认证必须为本法人（负责人）所拥有或被授权使用；

(5)▲投标人应仔细阅读招标文件的所有内容，按照招标文件的要求提交投标文件，并对所提供的全部资料的真实性承担法律责任；

(6)▲投标人在投标活动中提供任何虚假材料，其投标无效，并报监管部门查处；中标后发现的，中标人须依照《中华人民共和国消费者权益保护法》第 49 条之规定双倍赔偿采购人，且民事赔偿并不免除违法投标人的行政与刑事责任。

（二）采购文件

1. 采购文件的组成

(1)采购文件共分为六部分，其内容如下：

第一章 招标公告

第二章 投标须知前附表及投标须知

第三章 采购内容及要求

第四章 合同主要条款

第五章 评标办法

第六章 投标文件相关格式

(2)除上条 1.1 内容外，采购人在规定时间前，以书面形式发出的对采购文件的澄清或修改内容，均为采购文件的组成部分；

(3)投标人如在法律法规规定的时间内逾期对采购文件提出异议的，采购人可不予受理、答复。

2. 采购文件的澄清与修改

(1)采购人对采购文件进行必要的澄清或者修改的，在发布招标公告的网站上发布更正公告。澄清或者修改的内容可能影响投标文件编制的，更正公告在投标截止时间至少 15 日前发出；不足 15 日的，顺延提交投标文件截止时间；

(2)更正公告为采购文件的组成部分，一经在网站发布，视同已通知所有采购文件的收受人，不再采用其它方式传达相关信息，若因未能及时了解上述网站上发布的相关信息而导致的一切后果自行承担；

(3)如更正公告有重新发布电子采购文件的，投标人应下载最新发布的电子采购文件制作投标文件；

(4)投标人在规定的时间内未对采购文件提出疑问、质疑或要求澄清的，将视其为无异议。对采购文件中描述有歧义或前后不一致的地方，评审小组有权进行评判，但对同一条款的评判应适用于每个投标人。

（三）投标文件

1. 总体要求

(1)投标人应在认真阅读采购文件所有内容的基础上，按照采购文件的要求编制完整的投标文件。投标人应按本文件中提供的文件格式、内容和要求制作投标文件。投标文件内容不完整、编排混乱导致采购文件被误读、漏读或者查找不到相关内容的，是投标人的责

任；

(2)投标人必须保证投标文件所提供的全部资料真实可靠，并接受采购人对其中任何资料进一步审查的要求。投标文件中所有复印资料都须加盖单位公章（电子签章）；

(3)投标文件须对采购文件中的内容做出实质性和完整的响应，否则其投标将被拒绝。如果投标文件填报的内容资料不详，或没有提供采购文件中所要求的全部资料及数据，将会导致投标被拒绝；

(4)投标人已明知采购期间或之后企业将发生兼并改制，或提供的产品将停产、淘汰，及其他应当告知采购人可能影响采购项目实施或损害采购人利益的信息，必须在投标文件中予以特别说明，否则，采购人可以拒绝其投标文件；

(5)由于字迹模糊或表达不清引起的后果由投标人负责。

2. 投标文件的语言及度量衡单位

(1)除采购设备有关专用名称、型号外，投标文件与招标有关的所有文件说明均应使用中文；

(2)除采购项目规范另有规定外，投标文件使用的度量衡单位，均采用中华人民共和国法定计量单位。

3. 投标文件的编制

(1)投标文件由【资格审查文件】、【技术商务文件】和【报价文件】三部分组成，其中“资格审查文件”“技术商务文件”部分不得包含与本次项目有关的报价，否则作无效标处理。电子投标文件中须加盖公章部分均采用 CA 签章。

(2)【**资格审查文件**】包括但不限于以下内容：

▲①供应商基本情况表（格式见附件）；

▲②法定代表人身份证明或法定代表人授权委托书（格式见附件）；

▲③有效期内的营业执照（或事业法人登记证书或其它工商等登记证明材料）扫描件；

▲④符合参加国企采购活动应当具备的一般条件的承诺函（格式见附件）；

▲⑤联合体协议书（如有）

(3)【**技术商务文件**】包括但不限于以下内容：

①评分索引表（格式见附件）；

▲②投标函（格式见附件）；

③业绩一览表（格式见附件）；

④投标人按照评分标准要求提供的相应资料；

⑤投标人认为需要的其他内容（格式自拟）。

(4)【**报价文件**】包括但不限于以下内容：

▲①开标一览表；

▲②报价明细表；

③投标人认为需要提供的其他相关资料（如有）。

4. 投标文件的编制格式及说明

(1)请投标人在编制投标文件时仔细阅读本采购文件及其他辅助资料，根据本采购文件中评标原则及评分标准中所列内容结合自身情况据实提供相关资料。所提供的各种证书、证件、证明、执照须加盖电子签章并制作在投标文件内；

(2)投标文件应包括规定的内容，投标人提交的投标文件应当按采购文件要求提供的格式（格式可以按同样格式扩展）编制；采购文件未提供标准格式的，由投标人自行编写；

(3)投标人应严格按照采购文件规定的顺序编制目录，编排混乱或未按采购文件所提供的统一格式编写与漏项而导致投标文件被误读或查找不到有效文件由投标人承担风险；

(4)▲授权委托书、投标函、必须按规定盖章或签字。

以上内容未提供格式的，请投标人格式自拟。

5. 投标报价

(1)本项目最高限价：19100 万元，投标人报价超过最高限价、最高单价限价的作无效标处理；

(2)本项目投标报价包含人工费、交通费、餐费、材料费、税金、政策性风险和提供伴随服务等完成本项目的一切含税费用。如有合同费用漏项，视同已包含在其项目中，合同单价不做调整。投标人的投标报价为投标人所能承受的一次性最低报价。在合同服务期间内不得违反国家相关政策规定。采购文件未列明，而投标人认为必需的费用也需列入报价。

中标人应列入而未列入其中的费用，均视为已包含在内，风险由中标人承担。中标人不得以遗漏或疏忽为由向采购人主张增加费用或开支；

(3)投标人必须按第六章投标文件格式附件中的开标一览表（报价明细表）内容填写单价、合价和总价，并由法定代表人或授权代表签字或盖章；

(4)开标一览表及报价明细表上的价格须以人民币报价，以其它货币报价的投标将不予接受。

(5)采购人不接受任何选择报价，只允许一个报价；

(6)投标人应根据要求报价，报价单中不得漏填项目。

6. 投标文件的份数和签署

(1) 投标人应按本采购文件规定份数上传投标文件；

(2) 投标人应根据采购文件要求，在投标文件适当的位置填写投标人全称并加盖印章，同时签署投标人代表的全名。投标文件必须由投标人代表签字或盖章；

(3) 投标文件不得涂改和增删，如有修改错漏处，必须由同一投标人加盖公章；

(4) 投标文件因字迹潦草或表达不清所引起的后果由投标人负责；

(5) 投标文件的签章：投标文件应由投标人法定代表人或其授权代表签字（或盖章），并加盖投标人电子签章。投标人均应使用 CA 数字证书加盖投标人的单位电子印章、法定代表人个人电子印章，上传至衢州市阳光交易服务平台，作为投标文件正本，其余详见投标人须知前附表。

（四）投标有效期

1. 投标有效期见本采购文件中前附表所规定的期限，在此期限内，凡符合采购文件要求的投标文件均保持有效。

2. 在特殊情况下，采购人在原定投标有效期内，可以根据需要以书面形式向投标人提出延长投标有效期的要求，对此要求投标人须以书面形式予以答复。投标人可以拒绝投标采购人这种要求，但同意延长投标有效期的投标人既不能要求也不允许修改其投标文件。

（五）投标响应

1. 投标文件的上传和递交

(1) 投标人应在投标文件截止时间前（以上传完成时间为准）将由制作工具制作生成的电子加密投标文件（.QZCGTF）成功上传递交至衢州市阳光交易服务平台（<https://qzygjy.com/TPBidder/memberLogin?type=13>），否则投标无效。

2. 投标文件的修改与撤回

(1) 投标人应当在开标响应截止时间前完成投标文件的上传、递交，并可以补充、修改或者撤回投标文件。补充或者修改投标文件的，应当先行撤回原文件，补充、修改后重新上传、递交。开标响应截止时间前未完成上传、递交的，视为撤回投标文件。开标响应截止时间后递交的投标文件，“衢州市阳光交易服务平台”将予以拒收；

(2) 开标响应截止时间后，投标人不得撤回、修改《投标文件》。

（六）开标程序

1. 开标形式

采购代理机构将按照采购文件规定的时间通过“衢州市阳光交易服务平台”组织开标、

开启投标文件，所有投标人均应当准时在线参加。

2. 开标准备

(1)开标的准备工作由采购代理机构负责落实；

(2)采购代理机构将按照采购文件规定的时间通过“衢州市阳光交易服务平台”组织开标、开启投标文件，所有投标人均应当准时在线参加。投标人如不参加开标的，视同认可开标结果，事后不得对采购相关人员、招标过程和开标结果提出异议，同时投标人因未在线参加开标而导致投标文件无法按时解密等一切后果由投标人自己承担。

3. 开标原则

(1)采购代理机构按本采购文件投标人须知前附表规定的时间和地点开标，投标人未准时参加电子开标的，不得对采购相关人员、开标过程及结果提出异议；

(2)开标时出现的无效采购文件，不予评标。

3. 开标流程

(1)至投标截止时间

采购代理机构（或公证处工作人员）宣布开始开标，宣布开标项目名称等情况，公布在投标截止时间前受理的投标文件的供应商名称。

(2)供应商解密

供应商解密时间：投标文件开启时间到后，采购代理机构（或公证处工作人员）宣布开始解密，30分钟内供应商应完成投标文件的解密。供应商解密方式：投标人自行登录衢州市阳光交易服务平台不见面开标大厅（<https://qzygjy.com/BidOpening/bidopeninghallaction/hall/login>）——投标人身份——我的项目——选择标段——待代理开启解密后进行解密操作，投标人在规定的时间内都已完成解密，则系统自动结束解密；供应商因自身原因未在规定时间内完成解密，则默认自动放弃。采购代理机构导入投标文件成功后进入评标流程。

(3)供应商使用生成电子加密投标文件的CA数字证书解密投标文件；

(4)采购响应文件解密完成后，开标系统公布供应商名称及其他内容。投标报价将在技术商务文件评审结束后公布。

(5)进入评标环节，首先对解密成功的供应商进行资格审查，然后对通过资格审查的供应商进行技术商务文件评审，公布技术商务文件得分情况。

(6)供应商确认

唱标完成后，供应商可通过衢州市阳光交易服务平台不见面开标大厅系统对唱标结果

进行确认，未在开标结束前完成在线确认的供应商，衢州市阳光交易服务平台不见面开标大厅系统将视作自动确认。

供应商对开标过程有异议的，应通过衢州市阳光交易服务平台不见面开标大厅系统的“开标异议文字提问”按钮进行异议，采购人通过衢州市阳光交易服务平台不见面开标大厅系统文字答复，供应商提出异议的时间截止至开标结果公布后 5 分钟。

(7)评标结束后，采购代理机构（或公证处工作人员）宣布中标候选人。采购代理机构（或公证处工作人员）宣布开标会议结束。

4. 开标特别说明

(1)开标解密使用供应商上传的电子投标文件；

(2)因供应商原因（包括供应商自主选择的 CA 证书、电脑环境、网络等），造成其电子投标文件未解密的，或投标文件解密了，但投标文件无法识别、读取的，视为撤销其投标文件；

(3)供应商必须使用生成电子投标文件的 CA 数字证书解密电子投标文件。

特别说明：如遇“衢州市阳光交易服务平台”电子化开标或评标程序调整的，按调整后程序执行。

（七）投标人资格审查

1. 评审小组首先依法对各投标人的资格进行审查，审查各投标人的资格是否满足采购文件的要求。评审小组对投标人所提交的资格证明材料仅负审核的责任。如发现投标人所提交的资格审查文件不合法或与事实不符，采购人可取消其中标资格并追究投标人的法律责任。

2. 投标人提交的资格证明材料无法证明其符合采购文件规定的“投标人资格要求”的，评审小组将对其作资格审查不通过处理（无效投标），并不再将其投标进行后续评标。

3. 单位负责人为同一人或者存在直接控股、管理关系的不同投标人参加同一合同项下的采购活动的，相关投标人均作资格无效处理。

（八）无效标条款

1. 有下列情况之一的，对投标人作无效标处理。

(1)不具备采购文件规定资格要求；

(2)获取采购文件的投标人与参加开标投标人发生实质性变更的且未提供有效证明的；

(3)在“资格审查文件”“技术商务文件”中出现投标报价的；

(4)采购文件中有▲处条款投标人未作实质性响应的；

- (5)提供虚假材料谋取中标的；
- (6)投标报价超过采购预算价或最高限价的；
- (7)资格审查文件不全的，或者不符合采购文件标明的资格要求的；
- (8)投标人在投标报价计算或表达上有错误时，投标人不接受修正后报价的；
- (9)明显不符合采购文件中主要技术规格、技术标准的（例如关于“▲”条款及特别说明的）；
- (10)投标文件含有采购人不能接受的附加条件的；
- (11)投标文件载明的采购项目完成期限超过了采购项目文件规定的期限；
- (12)投标人有围标串标行为或明显串标嫌疑的；
- (13)不同投标人的投标文件制作机器码或创建标识码一致的（投标文件制作机器码一致是指 MAC 地址、CPU 序列号、硬盘序列号、主板序列号全部一致或制作 IP 地址、上传 IP 地址等与此电脑相关的硬件标识号码中有一个一致）
- (14)不符合法律法规和采购文件规定的其他实质性要求的。

（九）废标的情形

1. 采购中，出现下列情形之一的，应予废标：

- (1)符合专业条件的供应商或者对采购文件作实质响应的供应商不足 3 家的；
- (2)出现影响采购公正的违法、违规行为的；
- (3)投标人的报价均超过了采购预算，采购人不能支付的；
- (4)因重大变故，采购任务取消的。

废标后，采购人应当将废标理由通知所有投标人；除采购任务取消情形外，应当重新组织招标。

（十）评标程序

1. 评审小组

(1)采购代理机构和采购人将根据采购货物或服务的特点依法组建评审小组，评审小组对采购文件进行审查、询标、评议和推荐中标候选人；

(2)在评标期间，若有需要投标人应派代表参加询标。

2. 评标流程及内容

本项目具体的评标事务由评审小组负责，评标流程及内容如下：

(1)评标前准备

①由评标专家推选评审小组组长，采购人代表不得担任评审小组组长。

②由评审小组组长召集所有评审小组成员阅读采购文件及相关补充、质疑、答复文件、项目书面说明等材料，熟悉采购项目基本情况、项目技术规范和服务要求、合同主要条款、投标文件无效情形、评标办法、评标标准，以及其他与评标有关的内容。

(2)投标文件的初步审查、符合性审查

对所有通过资格审查的投标人的投标文件进行初步审查，审查、评价投标文件是否符合采购文件的商务、技术、服务等实质性要求。

评审小组首先对所有通过资格审查的投标人的投标文件进行符合性审查，审查每份投标文件是否实质上响应了采购文件的要求（实质性响应的投标文件是指投标文件符合采购文件规定的实质性内容、条件和规定）。

3. 投标文件的澄清、说明或补正

(1)对于投标文件中含义不明确、同类问题表述不一致或者有明显文字和计算错误内容的，评审小组将以书面形式（或通过“衢州市阳光交易服务平台”在线询标）的形式要求投标人在规定的时间内作出必要的澄清、说明或者补正，投标人澄清、说明或补正时间为30分钟。

(2)投标人的澄清、说明或者补正应当采用书面（或通过“衢州市阳光交易服务平台”在线答复）形式提交，并加盖公章，或者由法定代表人或其授权的代表签字。投标人的澄清、说明或者补正不得超出投标文件的范围或者改变投标文件的实质性内容。

4. 投标文件错误的修正

(1)投标文件如果出现计算或表达上的错误，修正错误的原则如下：

①投标文件中开标一览表内容与投标文件中相应内容不一致的，以开标一览表为准。

②投标文件的大写金额和小写金额不一致的，以大写金额为准；

③单价金额小数点或者百分比有明显错位的，应以开标一览表的总价为准，并修改单价；

④总价金额与单价汇总金额不一致的，以单价金额计算结果为准。

注：同时出现两种以上不一致的，按照前款规定的顺序修正，修正后的报价需经投标人确认后产生约束力，投标人不确认的，其投标无效。

(2)对不同文字文本投标文件的解释发生异议的，以中文文本为准。

5. 评标

(1)评定原则：根据符合采购需求、质量和服务等要求，综合评标确定中标人。

(2)投标文件的澄清：在评标期间，评审小组可要求投标人对其投标文件进行澄清，

但不得寻求、提供或允许对投标价格等实质性内容做任何更改。有关澄清的要求和答复均应以书面形式提交。

(3)评标报告：评审小组完成评定后，向采购人提交经各评审小组成员签字的评定结果报告，并按评定办法推荐中标候选人。

6. 可中止电子交易活动的情形

采购过程中出现以下情形，导致电子交易平台无法正常运行，或者无法保证电子交易的公平、公正和安全时，采购代理机构可中止电子交易活动：

- (1)电子交易平台发生故障而无法登录访问的；
- (2)电子交易平台应用或数据库出现错误，不能进行正常操作的；
- (3)电子交易平台发现严重安全漏洞，有潜在泄密危险的；
- (4)病毒发作导致不能进行正常操作的；
- (5)其他无法保证电子交易的公平、公正和安全的情况。

出现前款规定情形，不影响采购公平、公正性的，采购代理机构可以待上述情形消除后继续组织电子交易活动；影响或可能影响采购公平、公正性的，应当重新采购。

7. 保密

(1)公开开标后直到宣布授予中标人合同为止，凡属于审查、澄清、评估和比较投标的有关资料且与授予合同有关的信息都不得向任何投标人或与上述评标过程无关的人员透露。

(2)投标人对评标、比较或授予合同决定的过程施加影响的企图和行为，都可能导致其投标被拒绝。

(十一) 中标结果

1. 中标结果公告

(1)确定中标人后，采购代理机构在衢州市阳光交易服务平台 (<https://qzygjy.com/>) 上及公告发布的媒体中，进行中标结果公告，公告期限为 1 个工作日。

(2)中标人因自身原因放弃中标或因不可抗力不能履行合同的，经质疑，采购人审查确定因中标人在本次采购活动中存在违规行为或其他原因使质疑成立的，采购人组织重新招标。

2. 质疑和投诉

根据《衢州市国资委关于印发衢州市国有企业采购管理办法（试行）的通知》（衢国资发〔2020〕36号）、《中华人民共和国政府采购法》的规定，采购投标人可以依法提起

质疑和投诉。

2.1 投标人询问

投标人对采购活动事项有疑问的，可以向招标代理机构提出询问，招标代理机构在7个工作日内做出答复，但答复的内容不得涉及商业秘密。

2.2 投标人质疑

2.2.1 投标人认为招标文件、采购过程和中标、成交结果使自己的权益

受到损害的，可以在知道或者应知其权益受到损害之日起七个工作日内，以书面形式向招标代理机构提出质疑。逾期不予受理。

投标人应知其权益受到损害之日，是指：

(1)对可以质疑的采购文件提出质疑的，为收到采购文件之日或采购文件公告期限届满之日；

(2)对采购过程提出质疑的，为各采购程序环节结束之日；

(3)对中标结果提出质疑的，为中标结果公告期限届满之日。

2.2.2 投标人质疑应当有明确的请求和必要的证明材料，否则视为无效质疑，不予受理。投标人提交的质疑书需一式三份，由法定代表人（负责人）签字（或盖章）并加盖单位公章。质疑书至少应包括下列主要内容：

(1)质疑人的名称、地址、邮政编码、联系人、联系电话，以及被质疑人名称及联系方式；

(2)被质疑采购项目名称、编号及采购内容；

(3)具体的质疑事项及事实依据；

(4)认为自己合法权益受到损害或可能受到损害的相关证据材料；

(5)提出质疑的日期。

2.3 招标代理机构应当在收到投标人的书面质疑后七个工作日内作出答复，并以书面形式通知质疑投标人和其他与质疑处理结果有利害关系的采购当事人，但答复的内容不得涉及商业秘密。

2.4 投标人投诉

质疑人对招标代理机构的答复不满意或者招标代理机构未在规定的时间内作出答复的，可以在答复期满后十五个工作日内向采购人提出投诉，逾期不予受理。质疑人对采购人答复不满意的可以选择根据相关法律法规提起民事诉讼。

（十二）法律责任

1. 投标人有下列情形之一的，将上报相关监管部门处以采购项目中标金额千分之五以上千分之十以下的罚款，列入不良行为记录名单，在一至三年内禁止参加采购活动，并予以公告，有违法所得的，并处没收违法所得，情节严重的，由工商行政管理机关吊销营业执照；构成犯罪的，依法追究刑事责任：

- (1)提供虚假材料谋取中标的；
- (2)采取不正当手段诋毁、排挤其他投标人的；
- (3)与采购人、采购代理机构、其他投标人恶意串通的；
- (4)向采购人、采购代理机构行贿或者提供其他不正当利益的；
- (5)在开标过程中与采购人进行协商谈判、不按照采购文件和中标人的投标文件订立合同，或者与采购人另行订立背离合同实质性内容的协议的；
- (6)拒绝有关部门监督检查或者提供虚假情况的；

（十三）授予合同签订资格

1. 中标通知书

- (1)在公告中标结果的同时，采购人或者采购代理机构应当向中标人发出中标通知书。
- (2)中标通知书是中标人与采购人签订合同的凭证，是授予合同签订资格的合法依据。
- (3)中标通知书发出后，采购人不得违法改变中标结果，中标人无正当理由不得放弃中标。

(4)中标人按《中标通知书》指定的时间、地点与采购人直接签订合同后生效。在有合理证据证明中标人在投标过程中承诺的内容不能实质响应的，采购人有权拒签合同。

2. 合同的签订

(1)采购人应当自中标通知书发出之日起 30 日内，按照采购文件和中标人投标文件的规定，与中标人签订书面合同。所签订的合同不得对采购文件确定的事项和中标人投标文件作实质性修改。

(2)采购合同应当包括采购人与中标人的名称和住所、标的、数量、质量、价款或者报酬、履行期限及地点和方式、验收要求、违约责任、解决争议的方法等内容。

(3)招标文件、澄清文件、投标文件等，均为签订合同的依据。中标人接到中标通知书后在规定的时间内与采购人签订合同。

(4)中标人不遵守投标文件的要约、承诺，擅自修改投标文件的内容或在接到中标通知书规定的时间内，借故拖延、拒签合同者，采购人将取消该投标人的中标资格。

(5)采购人与中标人应当根据合同的约定依法履行合同义务。

(6)采购合同的履行、违约责任和解决争议的方法等适用中华人民共和国民法典。

(7)中标人应当按照合同约定履行义务完成项目。

3. 代理服务费及其他费用（以人民币元收取）

(1)代理服务费由中标人支付给代理机构。

本次采购代理服务费用按国家标准《计价格【2002】1980号文件》16%计取，按服务招标计算，不足2000元按2000元计算，由中标人领取中标通知书前支付给采购代理机构。收费标准如下：

费 率 服务 类型 中标金额（万元）	货物招标	服务招标	工程招标
100以下	1.5%	1.5%	1.0%
100-500	1.1%	0.8%	0.7%
500-1000	0.8%	0.45%	0.55%
1000-5000	0.5%	0.25%	0.35%
5000-10000	0.25%	0.1%	0.2%
10000-100000	0.05%	0.05%	0.05%
100000以上	0.01%	0.01%	0.01%

费用不在报价中单列，请各供应商在报价时考虑。

4. 解释权

凡涉及本次文件的解释权均属于衢州市数字产业发展有限公司和衢州市开成工程造价咨询事务所有限公司。

第三章 采购内容及要求

一、采购内容和技术要求

(一) 主要采购内容

1. 衢州市政务云服务（XC 部分）采购内容

1) 基础云资源服务

基于“两地三中心”架构体系，建设基于自主可控关键核心技术的云平台，提供计算、存储、网络、国产数据库、国产中间件、国产操作系统、云原生数据库等服务。

2) 应用服务

提供企业级分布式应用、应用实时监控、云服务总线、流量防护、性能测试、消息队列、容器服务、API 网关等服务。

3) 大数据服务

提供大数据计算、实时计算、搜索服务、智能报表、实时数仓、数据分析等大数据相关服务。

4) 容灾备份服务

提供异地备份服务。

5) 安全服务

提供网络安全（漏洞扫描、主机安全防护、WEB 应用防火墙等）、应用安全（代码审计、高危隐患和安全事件预警等）、数据安全（数据库权限管控系统、数据库审计等）、攻防演练（攻防演练服务、重要活动时期安全保障等）、渗透服务等安全服务。

6) 机柜托管服务

提供机柜托管服务。

2. 衢州市政务云服务（非 XC 部分）采购内容

1) 基础云资源服务

提供云主机计算、块存储、对象存储、云数据库等基础云资源服务。

2) 大数据服务

提供大数据服务、大数据开发治理等服务。

3) 其他服务

提供云产品备份、分布式应用、主机托管等服务。

4) 安全服务

提供网络安全（漏洞扫描、云堡垒机、日志审计、WEB 防火墙等）、渗透服务、应用

安全（代码审计、主机安全防护等）、数据安全等服务（数据库权限管控、数据库审计、静态脱敏等）。

（二）容灾服务要求

结合《浙江省大数据发展管理局关于印发政务云灾备指南（试行）的通知》的要求，按照“两地三中心”（同城、异地两地，生产中心、同城容灾中心、异地备份中心三中心）总体架构进行设计。供应商建设多个云节点互为同城容灾中心，实现同城业务灾备。与已建省级政务云异地备份中心（金华）对接，实现异地数据备份，整体组成“两地三中心”架构。

异地数据级容灾备份服务，在供应商承建的云节点分别部署数据备份软件，按照《灾备指南》要求，将等保三级及以上业务系统数据通过数据备份软件，同步至省本级异地数据级容灾备份中心（设在金华市）。充分利用省本级已建在金华市的相关备份服务和专网通道能力。

（三）云服务指标要求

1. 云基础资源服务要求

服务区域划分要求，本次采购要求提供基于政务外网的政务云网络环境，同时提供满足对不同安全级别、不同业务、不同专网的需要。支持虚拟专有域功能（VPC），能够划分隔离的区域为特定的云租户提供云服务，区域内的资源与别的云租户完全隔离，完全为该云租户使用。各部门可接入政务云平台，实现与原有业务专网互通，IP 地址自定义划分，与云上其他局办业务隔离。

2. 资源管理要求

满足云租户对云资源清单、性能、使用率、运行状态、查询导出功能，能够提供对云资源进行监控、分析、告警等管理功能的各类操作；按照采购人要求提供相关业务接口及接口使用文档。

3. 互联网出口基本要求

云平台须为本项目租用的云主机提供公有 IP 地址，政务云网络的核心及出口基础设施要与政务外网匹配适应。

4. 信息系统安全基本要求

投标人须承诺云平台在验收前通过信息系统安全等级保护测评（三级及以上），并取

得公安机关颁发的备案证书。

（四）配套服务要求

1. 提供容灾管理服务、流量负载均衡服务；
2. 技术支持服务：含容灾咨询服务、容灾演练服务、运维服务；
3. 组建由云服务商、原厂（授权）技术服务商、安全厂商组成的云服务技术团队。

（五）自主可控关键核心技术要求

1. 应采用通过相关机构的安全可靠测评的服务器搭建云平台底座，并且支持一云多芯；
2. 除采购方特殊要求外，物理服务器扩容和替换须采用通过相关机构的安全可靠测评的产品；
3. 云服务器须提供通过相关机构的安全可靠测评的操作系统。

（六）项目具体技术参数需求

1. 总体服务要求

指标项	规格要求
资源可用性	本指标定义为云服务商应承诺在合同期内每年用户云服务业务可用时间的概率，即每年实际可用时间/（实际可用时间+不可用时间）。
	云主机、云数据库、对象存储、负载均衡、云网络、大数据、云安全、数据备份。
	云服务商初期可分期按需建设，以适应业务需求。
服务交付	各项云服务交付时应主动提供操作手册，并协助解决平台层面问题。
数据存储持久性	本指标定义为云服务商承诺在合同期内数据保存不丢的概率，即每年完好数据/（完好数据+丢失数据）。
	云主机、云数据库、对象存储、负载均衡、云网络、大数据、云安全、数据备份。
运营能力	对用户开通的服务进行计量计费，按月、季度、年向用户提供完整的记账单。
	实现与 IRS 对接服务，包括：资源申请、升降配、释放；IRS 资源自动开通；IRS 资源监管。

指标项	规格要求
标准规范	采用统一平台进行集群资源管理，实现集群内 CPU、内存、磁盘和网络资源高效地使用。
	根据应用对资源进行全局调度，提高资源的利用率。
	采用自动故障切换提高系统整体的可用性。
	采用统一的安全措施，保证用户数据的安全性。
	采用统一运维的方式，提高系统的安全并降低成本。
扩展规模	支持在线集群扩容和应用服务的在线升级。
资源管理	需提供计算存储设备，网络设备和安全设备等物理设备的管理功能，提供全局拓扑。
	需提供完整的 IaaS 云服务，具体应包括：云计算、云存储、云网络、云数据库、负载均衡、云安全等。实现政务云平台各资源配置及利用率情况与衢州市基础设施管控平台对接。
	需提供政务云平台资源使用日常监管工作服务，对于资源使用率低于 CPU15%、内存 35%标准的系统，应及时通知整改，长期未整改项目应配合采购人要求，对系统进行优化处理。本项指标考核纳入服务绩效考核中。
资源调度	需提供资源调度能力，且具备高可扩展性。
	具备自动检测故障，保证作业稳定可靠运行完成。
运维监控管理要求	需提供每季度提供至少 1 次运维服务报告，对运维服务进行总结，提供输出《季度服务报告》。
	需提供重要活动时期云平台原厂（原厂认证授权），在保障期前，对平台环境进行深度检查，发现问题并进行问题修复。在容灾、可用性、紧急扩容预案等方面提供参考方案。
	每年需提供至少 4 次平台深度巡检服务。
云安全管理要求	平台具备安全监控功能，支持云平台本身的安全监控，包括攻击防护、安全告警和脆弱性等平台安全基线检查功能。
	需具备云主机安全配置监控：支持显示各云主机的公网 IP 地址、所属部

指标项	规格要求
	门/单位、所属 VPC、运行状态、操作系统、安全告警、脆弱性风险、攻击、Agent 状态、磁盘信息、快照信息、内存、磁盘、安全组等；以及单资产详细告警、脆弱性和攻击风险列表。支持查询及查询结果导出。
云平台等保合规	须通过三级等级保护测评（测评得分不低于 90 分），并提供佐证材料。
	在服务能力验收后 9 个月内，须通过国家密码应用安全性测评，并提供佐证材料。

2. IDC 机房要求

需提供专用 IDC 机房服务，具体要求见下表：

指标项	规格要求
机房地點	机房物理地址在衢州市的机房服务。
动力保障	2 路市电接入机房。
	2N 系统架构 UPS 配置，确保供电安全。
	配置同等容量柴油发电机，油量储备可以支持发电机满载运行 8 小时。
	所有机柜均由两套不同的 UPS 系统提供双路供电。
空调系统	恒温恒湿机，温度保持在 20-25 度，相对湿度保持在 40%~55%。
	空调主机双路供电，自动切换，保障无市电情况下的持续运转。
消防系统	符合分区域消防联动系统，保障机房运行安全。通过消防安全评估。
防雷系统	需通过防雷系统检测，满足标准要求。
网络资源	保证网络高可靠性、高可用性、高扩展性、冗余性，要求采用双核心和接入两层扁平化的组网架构，核心接入之间万兆捆绑互联。
	满足服务期内衢州市、县两级部门（单位）对政务云平台中业务应用网络带宽、业务平稳、持续不间断运行等应用需要。具备与衢州市政务外网相连接的环境，政务云机房与政务外网提供传输波分网络对接互联，双链路。
物理和环境安全要求	政务云物理机房应符合等保、密评对机房安全管控要求。
其他要求	参考《绿色数据中心政府采购需求标准（试行）》的相关要求。

3. 衢州市政务云服务（XC 部分）技术要求

1) 基础服务

a. 云主机

指标项	规格要求
服务标准	根据用户的需求动态地创建和分配计算资源与存储资源。
服务特性	云主机创建。从创建到启动在 5 分钟以内。
	云服务器提供快照制作，快照回滚，自定义 image，动态升级，可以为每块磁盘创建快照。
	支持虚拟机故障切换，在线迁移；支持宿主机宕机迁移。
	主机之间网络访问逻辑隔离，支持创建和管理安全组；提供安全组的创建、修改、删除以及批量删除等功能。
	需提供丰富的 API 接口，包括资源的创建，删除，修改，查询，启动等操作。
	云服务器工作节点采用分布式高可用架构，保障云服务器的高可用性。
	支持资源开通时指定 IP 地址。
操作系统	提供主流的自主可控关键核心技术操作系统如：麒麟、统信等操作系统。

b. 块存储

指标项	规格要求
功能要求	支持在线扩展容量，扩容期间无需关闭虚拟机，无需卸载云盘；系统盘在线扩容不停业务。
	支持磁盘的创建、删除、卸载、扩容、挂载、查询、初始化等功能。
总体要求	为云主机提供的低时延、持久性、高可靠性的数据块级存储设备。
安全性	支持分布式 EC 或三副本数据冗余保护，三副本模式下，数据三副本支持分布在 3 个机柜或 3 对接入交换机上。

c. 对象存储

指标项	规格要求
服务标准	提供基于三副本或 EC 校验模式的数据多重冗余备份，保证数据安全。

指标项	规格要求
服务特性	支持 RESTful API 接口，通过开发工具包 SDK 或直接通过 RESTful API 进行对象存储操作。
	提供 key-value 键值对形式的对象存储服务。
	具备多用户隔离机制。
	提供标准 RESTful 协议的 API 接口以及多语言的 SDK。
	提供服务端数据加密。
	支持对象简单上传/下载/删除/复制。
安全访问	支持 Bucket 级别的 ACL。
	支持服务器端的加密功能，用户能够使用密钥管理系统上创建的密钥进行加密。

d. 负载均衡

指标项	规格要求
服务要求	支持四层负载均衡和七层负载均衡； 支持集群高可用架构，支持动态扩展。
服务特性	协议支持：提供四层（TCP 协议和 UDP 协议）和七层（HTTP 和 HTTPS 协议）的负载均衡服务。
	应提供多种转发规则，满足不同业务场景的要求：域名、url 转发。
	健康检查：提供后端 ECS 实例的健康检查。负载均衡服务会自动屏蔽异常状态的 ECS 实例，待该 ECS 实例恢复正常后自动解除屏蔽。
	调度算法：支持轮询、最小连接数两种调度算法： 轮询：按照访问次数依次将外部请求依序分发到后端 ECS 实例上。 最小连接数：连接数越小的后端服务器被轮询到的次数（概率）也越高。
	访问控制：支持白名单访问控制。通过添加负载均衡监听的访问白名单，仅允许特定 IP 访问负载均衡服务。
可靠性	管理节点采用全冗余架构。

e. 弹性公网IP

指标项	规格要求
服务要求	支持将 EIP 与 VPC 内的实例进行绑定，使该实例可以与外网通信。
	支持修改 EIP 带宽。
	支持随时将 EIP 与实例进行解绑。

f. 国产WEB中间件

指标项	规格要求
服务要求	提供通过相关机构的安全可靠测评的主流国产 WEB 中间件产品。

g. 国产操作系统

指标项	规格要求
服务要求	提供通过相关机构的安全可靠测评的主流国产操作系统。

h. 国产数据库

指标项	规格要求
服务要求	提供通过相关机构的安全可靠测评的主流国产数据库软件产品。

2) 存储服务

a. 数据库存储备份

指标项	规格要求	
功能要求	支持主流数据库类型备份。	
	支持整个实例、多个数据库、单个数据库、多张表、单表、视图、存储过程、触发器、函数备份。	
	支持备份频率、周期、开始时间、并行线程数等备份计划配置。	
	支持全量和增量备份保留时长配置到期自动删除。	
	支持计划外手动发起全量备份。	
	支持恢复时间点配置。	
	支持恢复目标库新建实例或者使用已有实例。	
	外置存储池管理	支持备份到三方存储池，包括文件存储、对象存储。
	批量管理数据源	支持批量自动接入新增数据源实例。
	批量配置备份计划	支持相同的数据库类型和相同的备份类型的批量配

	置备份计划。
总体要求	数据库备份服务是为数据库提供连续数据保护、低成本的备份服务，它可以为多种环境的数据提供强有力的保护，包括企业数据中心，数据库备份拥有一套完整的数据备份和数据恢复解决方案，具备增量备份以及精确到秒级的数据恢复能力。
安全性	支持多种加密技术保护备份数据存储安全。

b. 日志服务

指标项	规格要求
服务标准	针对日志类数据的一站式服务，提供日志数据的采集、查询、分析、消费等多种功能。

3) 网络服务

a. NAT 网关

指标项	规格要求
服务要求	平台提供 NAT 网关服务，支持 NAT（SNAT 和 DNAT）功能。

b. 高速通道

指标项	规格要求
服务要求	平台提供高速通道服务，用于在云上的不同网络环境间实现高速、稳定、安全的私网通信，包括跨地域/跨用户的 VPC 内网互通、专线接入。

c. DNS 解析

指标项	规格要求
功能要求	VPC 私有域名解析支持租户隔离的功能特性，支持权威域名的添加、修改、备注、删除、批量删除操作的功能，同时也支持根据关键字进行模糊查询，针对每个 VPC 都可以提供定制化的私有网络 DNS 解析服务配置，实现 VPC 粒度的租户隔离功能。
	内网权威域名管理和解析：支持 IPV6 域名解析服务。
	内网权威域名管理和解析：支持域名主机记录的添加、删除和修改操作的功能，支持的记录类型包括 A、AAAA、CNAME、NS、MX 等。

总体要求	VPC 私有域名转发配置管理和解析：支持域名级别的转发操作，将特定域名的解析操作转发到其他 DNS 服务器上解析；支持默认转发功能的配置，将本地不存在的所有域名的解析操作全部转发到其他 DNS 服务器上解析。
------	----------------------------------------------------------------------------------------------------------

d. VPC

指标项	规格要求
服务标准	在所提供的云平台构建出一个隔离的网络环境，客户完全掌控自己的虚拟网络，包括选择自有 IP 地址范围、划分网段、配置路由表和网关等。
服务特性	使用隧道技术达到与传统 VLAN 相同隔离效果。 按需配置网络设置、软件定义网络，管理操作实时生效。 支持使用高速通道实现跨地域/跨用户的内网互通和物理专线接入。 支持使用 NAT 网关进行 DNAT/SNAT 转发。 通过 NAT 网关支持灵活的 DNAT/SNAT 转发。
服务能力	可以通过交换机将专有网络的私有 IP 地址划分成一个或多个子网。根据业务需求配置虚拟路由器的路由规则，管理专有网络流量的转发路径。

4) 云数据库服务

a. 云数据库-类型 I (兼容 MySQL、Oracle)

指标项	规格要求
安全要求	支持数据库内部的加密存储、传输加密、访问白名单、Label security、安全审计、细粒度访问控制等安全特性。
功能要求	支持事务处理、MVCC 多版本控制、死锁机制，事务处理系统具备原子性、一致性、隔离性、持久性。
	兼容 MySQL、Oracle 常用语法和函数，支持 SQL92/SQL99/SQL2003 语法标准，覆盖 99.9%以上应用开发常用 SQL，包括存储过程、触发器、自定义函数、自定义类型等数据库对象。
	支持标准 SQL 语法，支持数据的多数据分片/分区的自动路由与聚合，支持跨库的复杂查询。

	支持数据库集群多点写入、读写分离。
	具备在线全量备份、在线增量备份的功能，支持任意时间点的备份还原操作，保证数据强一致、时间点强一致、不阻塞业务服务。
	支持大并发情况下的分布式事务，保证数据强一致和处理能力。
	提供图形化界面的数据库运维管理工具，具有可视化实时监控、自动化运维、报警、参数管理、集群管理、租户管理、日志管理、健康巡检等功能。
	软硬件适配能力：支持 x86、ARM 硬件平台、主流操作系统，以及国产操作系统麒麟、UOS 等；支持主流的中间件产品组件，支持异构芯片多集群混布，如同一个底座，可以同时部署 intel/海光/鲲鹏/飞腾，四个芯片的集群，复用同一套管控。
总体要求	具备高性能、高可用、可扩展的分布式关系型数据库。

b. 云数据库-类型 II（兼容 MySQL）

指标项	具体要求
可靠性指标	采用全冗余架构，无单点故障。
功能要求	提供自动化读写分离方案，提供手动配置流量分配比例。启动读写分离不需要重新配置数据库连接。
	支持秒级 DDL、并行 DDL、非阻塞 DDL。支持数据库级、表级数据恢复。
	兼顾性能和成本考量，提供丰富的数据库规格类型，包括独占物理资源规格、共享物理资源规格。
	支持 MySQL 交互协议，兼容市面上主流 MySQL 驱动，支持多语言接入，提供丰富的 MySQL 版本兼容性，支持 5.7、8.0。
总体要求	分布式数据库兼容 MySQL 协议和语法，支持分库分表、平滑扩容、服务升降配、透明读写分离和分布式事务等特性，具备分布式数据库全生命周期的运维管控能力。
安全性	支持根据 IP 白名单，或者 IP 组白名单形式控制数据库访问源。

c. 云数据库-类型 III（兼容标准 SQL）

指标项	规格要求
-----	------

指标项	规格要求
基本功能/性能	分布式数据库采用基于 Share-nothing 的 MPP 架构，支持横向扩展。
	支持主备形态、分布式形态集群模式，支持基于裸机和云主机形态进行部署，为不同业务场景提供灵活的部署形态选择。
	支持分布式事务强一致，保障数据一致性。
	支持灵活的分区管理操作，降低分区管理复杂度，支持分区创建、修改、删除。
	支持表空间管理，表空间用于管理数据对象，与磁盘上的一个目录对应。
	支持大对象类型，包括 clob、text、blob 类型，其中 text 和 blob 支持最大 1G。
	支持生成 WDR 诊断报告，用于快速诊断数据库内核性能问题。
	支持完善的安全防护能力，包括全密态加密、透明加密、SSL 加密、动态脱敏。
	支持 Oracle 数据库到分布式数据库在线迁移和数据库实时同步的云服务。提供数据全量和增量迁移工具，降低了数据库之间数据流通的复杂性，有效地帮助用户减少数据传输的成本。
服务安全	设置已删除实例保留天数，可设置范围为 1~7 天。
	支持将删除的实例，加入回收站管理。用户在回收站保留期限内的实例可以通过重建实例恢复数据。

d. 分布式关系型数据库

指标项	规格要求
基本功能/性能	兼容 MYSQL 协议和语法，支持自动化水平拆分。
	支持在线平滑扩缩容，服务能力线性扩展，透明读写分离。
	客户端支持：兼容数据库登录协议。
	支持外部数据源的增量和全量导入，帮助用户实现数据库平滑上云。
	支持分库分表按照逻辑库表导出。
	提供 sql 命令的方式查看物理、逻辑架构，展示慢查询等功能，可以帮助

指标项	规格要求
	迅速定位慢 SQL 问题。
	支持自动化数据拆分，支持字符串，日期，数字的多种拆分方案。
	提供完整的数据库运维监控系统，对数据库 IOPS，TPS，CPU 实时监控。
服务安全	采用分布式集群服务，无服务单点故障。
	支持存储层数据库白名单自动维护，通过白名单保证访问安全。

5) 中间件服务

a. 应用实时监控

指标项	指标子项	规格要求
易用性	交互大盘	支持基于数据集配置交互式大盘，大盘可动态刷新。
功能指标	编程语言支持	针对Java等语言开发的应用，支持通过探针方式提供应用监控，为Java等语言开发的应用安装Agent后，即可开始监控Java等语言开发的应用，无需代码侵入。
功能要求	依赖拓扑图	能统计出服务和服务的关联依赖图。
	外部调用监控	可以查看该应用的所有外部调用的请求数、响应时间、错误数及HTTP状态码信息。
	应用接口监控	支持应用接口的指标统计，包括请求数，响应时间和错误数等。
	应用标签能力	支持对应用进行标签分组与过滤。
	应用监控报警能力	支持默认提供应用各维度指标的报警，包括但不限于JVM、异常接口调用、应用调用类型统计、主机监控、数据库指标等应用监控的风险信息进行报警。
总体要求	自定义监控报警能力	支持基于用户自定义监控数据集指标的报警。
	应用节点监控	提供对于服务提供者以及消费者的集群以及单机的CPU，内存，磁盘、网络的监控并以图形化形式按照小时，天，周进行曲线展现。
	监控应用框架支持	支持基于主流同步、异步调用框架，如Spring Cloud，HTTP RESTful的分布式链路跟踪。

b. 消息队列

指标项	规格要求
服务标准	基于高可用分布式集群技术，提供消息订阅和发布、消息轨迹查询以及定时（延时）消息、资源统计等系列消息云服务，为分布式应用系统提供异步解耦、削峰填谷的能力，同时具备海量消息堆积、高吞吐、可靠重试等

	应用所需的特性。
服务特性	支持TCP等协议。
	<p>消息类型</p> <p>普通消息：消息队列MQ中无特性的消息，区别于有特性的消息。</p> <p>定时（延时）消息：允许消息生产者指定消息进行定时（延时）投递。</p> <p>事务消息：实现类似X/Open XA的分布事务功能，以达到事务最终一致性状态。</p> <p>顺序消息：允许消息消费者按照消息发送的顺序对消息进行消费。</p>
服务能力	消息查询：提供了三种消息查询的方式，分别是按Message ID、Message Key以及Topic查询。

c. 容器服务

指标项	规格要求
服务标准	容器服务（Container Service）是一种高性能可伸缩的容器管理服务，支持企业级Kubernetes容器化应用的生命周期管理。
服务特性	支持多集群管理，支持多集群的统一管控。
	<p>一站式容器生命周期管理：</p> <p>日志：支持容器实例日志查看和应用日志采集。</p> <p>监控：支持集群、节点、应用、容器实例层面的监控，为集群提供全方位监控大盘。</p> <p>集群管理：容器服务与云平台无缝对接，能够通过控制台实现集群的一键式自助创建和删除集群。</p>
	支持跨可用区高可用和灾难恢复。

d. API 网关服务

指标项	指标子项	规格要求
功能要求	协议支持	支持 HTTP2.0 协议、websocket、双向通信等。
	安全管控	支持多种访问控制方式,包括 IP 访问控制、参数访问控制。
	安全管控	支持流量限制，包括基础流控功能，如基于授权的流量控制，流控的时间区间支持秒、分钟、小时。

	请求转发	支持参数映射，可以从 HTTP 请求的各种位置上读取参数，并支持映射到后端不同的参数名、参数位置上；错误码映射，支持将后端应答中返回的非正常请求，映射为客户端期望的错误应答的场景。
	请求转发	支持参数路由，从应答或系统上下文中获取参数，并使用自定义的条件表达式对参数进行逻辑判断，满足条件后，支持对后端服务的定义与覆盖规则。
	集成能力	支持大数据平台作为后端服务，以 API 形式对外提供数据服务。
总体要求	API 全生命周期管理	覆盖 API 全生命周期管理，包括 API 设计、开发、测试、发布、运维监测、安全管控、下线等 API 各个生命周期阶段。

6) 大数据服务

a. 大数据计算服务

指标项	规格要求	
功能指标	节点调度	超大规模节点调度能力，具备单集群 30000 节点以上调度能力。为保证大数据集群具有高可扩展性。
	集群规模	采用分布式计算框架提供大规模数据存储与计算，可按需扩容。
功能要求	功能特性	支持 MapReduce 类型的分布式计算任务，支持 DAG 模式的作业处理方式。
	功能特性	支持多种计算框架如 SQL、MapReduce、Spark、Graph。
	功能特性	支持原生 Apache Spark 编程接口，用户可以使用 Spark 接口进行编程处理存储在大数据计算服务中的数据。
	功能特性	提供完整 RESTful API 的方式提供离线数据处理服务，提供 JAVA SDK，Python SDK，等编程接口，支持 JDBC 接口等系列用户开发工具和接口。

	功能特性	提供离线任务管理、监控告警的功能。
--	------	-------------------

b. 实时计算服务

指标项	规格要求
服务标准	提供实时流数据计算服务的通用计算平台。
	数据运维：提供以下运维监控功能：作业状态、血缘关系和属性参数。
	性能调优：支持手动和自动调优方式。
服务能力	强大的实时处理能力：单作业吞吐最高可达百万级别记录/秒。
	良好的流式开发体验：支持标准 SQL。

c. 大数据搜索与分析

指标项	规格要求
易用性	支持通过管控平台一键创建 Elasticsearch 集群、操作灵活便捷。
功能要求	提供界面友好的海量信息索引库及全文检索集群运维管理平台，可实时查看索引库及集群状态，支持基础指标的 Web 化展示。
	提供原生 Elasticsearch 的 API 编程接口，用于大数据搜索服务的数据导入，索引建立和数据检索。
	数据入库后，支持通过插件兼容 SQL 查询，支持条件组合灵活查询。
	集群规模可平行扩展。节点扩容过程平滑，不影响集群正常查询，不需要停服务。
总体要求	提供一个分布式的全文搜索引擎，实现数据搜索、数据分析等功能。
安全性	支持业务创建和使用一个或多个 Elasticsearch 集群，具备较为完善的权限认证与隔离机制，保障数据安全。

d. 大数据开发治理平台

指标项	规格要求
基础功能	为国产数据仓库/数据湖/湖仓一体等解决方案提供统一的全链路大数据开发治理平台。
数据集成	支持多数据源之间的数据接入和同步。

数据开发	通过 SQL 编辑器实现代码输入，包含关键字、函数、表、字段等信息；支持错误语法实时提示。
运维中心	支持调度系统诊断，完善调度系统作业的性能和稳定性。
数据质量	支持数据质量校验规则与调度系统结合，数据产出后立即触发任务调度，若配置的强规则校验失败，则将任务状态置为失败，避免脏数据对下游作业产生污染。
数据服务	服务编排：提供拖拽式、可视化的服务编排能力，支持用户按照业务逻辑，以串行、并行和分支等结构编排多个 API 及函数服务为工作流。
数据保护伞	分级管理：自定义数据安全等级。 数据脱敏：包含有敏感信息的数据库，对敏感信息进行动态遮蔽。
迁移助手	支持新建导出任务。

7) 容灾备份服务

产品名称	指标项	指标要求
异地备份服务	技术要求	1、提供云服务器、对象存储、文件存储、关系型数据库备份能力。
		2、支持自定义备份计划；支持创建、启动、停止备份计划；支持备份日志、备份记录查看和图形化备份统计视图；支持按备份策略执行备份。
		3、支持按备份记录或时间节点进行恢复；支持创建、启动、停止和查看恢复任务；支持查看恢复实例的日志信息。
传输专网	技术要求	各容灾中心分别部署 10G 专线（裸光纤）。

8) 安全服务

提供网络安全（漏洞扫描、主机安全防护、云堡垒机等）、应用安全（代码审计、高危隐患和安全事件预警等）、数据安全服务（数据库权限管控、数据库审计、动态脱敏等）、其他安全服务（攻防演练、渗透服务等），具体如下表：

安全产品	具体技术要求
漏洞扫描	支持对各种网络主机、操作系统、网络设备（如交换机、路由器、防火墙

	<p>等)、常用软件以及应用系统的识别和漏洞扫描;</p> <p>用户可自定义扫描端口范围、端口扫描策略等扫描选项;</p> <p>支持对各种网络主机、操作系统、网络设备(如交换机、路由器、防火墙等)、常用软件以及应用系统的识别和漏洞扫描;</p> <p>支持手动创建资产也可以批量导入资产,在资产管理页面可直接对单个资产或批量资产下发扫描任务;</p> <p>支持自定义扫描策略模板,可以将自定义策略模板导出备份,也可以导入备份的策略模板,能够对策略模板进行编辑、另存为新的模板;</p> <p>支持导出的报告类型≥5种,包括HTML、WORD、PDF、EXCEL、XML报告格式。</p>
主机安全防护	<p>支持防端口扫描,锁定恶意的端口扫描,并记录告警;</p> <p>支持病毒库、补丁库的离线升级及在线升级;支持管理平台、终端软件安装包、终端软件更新包、系统漏洞库、弱口令库的离线升级。</p> <p>支持按照防护类别筛选日志,包括:高级威胁、系统防护、网络防护、Web应用防护。</p>
WEB应用防火墙	<p>产品符合自主可控关键核心技术要求</p> <p>支持源地址识别,部署在SSL网关后面,能够解析到真实的访问者IP,并能对真实的IP进行防护和阻断。</p> <p>内置Webshell检测规则,可以对上传的文件内容进行检查,防止恶意Webshell文件上传,对已经上传的Webshell发起请求的行为进行拦截阻断。</p> <p>能够检测防止服务器导致的信息泄露行为,包括:目录信息泄露、服务器信息泄露、数据库信息泄露、源代码泄露等信息泄露行为。</p> <p>内置安全规则可有效识别Acunetix、nessus、WebScan、Webdump、AppScan等扫描器的扫描行为。</p> <p>支持对HTTP请求中URI、HOST、参数、参数名、请求头、Cookie、版本号、方法和请求体及HTTP响应的响应体等条件进行自定义正则。</p> <p>支持阻断、重定向、智能加黑名单、丢弃、告警、仅检测等动作。不同的</p>

	<p>防护规则，可以选择不同的防护动作及返回码，也可针对不同规则设置专属 URL 白名单。</p> <p>具有机器学习安全引擎，可以对用户 web 业务系统建立安全的访问模型，学习的内容包括 URL 地址、URL 请求参数等信息。</p> <p>支持智能识别攻击者，对网站链接发起攻击的 IP 地址进行自动锁定</p> <p>WAF 支持与 APT 产品联动实现对未知威胁的感知拦截。</p> <p>能详细记录攻击事件的 HTTP 请求头信息，含请求的 URL、UserAgent、POST 内容，cookie 等所有的请求头内容。</p> <p>支持报表导出为 Word、pdf、html 等多种格式。</p> <p>规则库支持手工、在线升级两种方式，在线升级可支持规则定时检查新版本和在线更新，确保 WAF 能够针对新型的、突发型的 Web 攻击进行防护。</p>
云堡垒机	<p>支持用户多角色划分功能，如系统管理员、部门管理员、运维员、审计管理员、密码管理员等，对各类角色需要进行细粒度的权限管理。支持自定义用户权限：</p> <p>混合云管理：支持标准适配多个云环境，包括阿里云、华为云、百度云、AWS、腾讯云等，支持同步云上主机信息至堡垒机；</p> <p>支持完善的自动改密安全保护机制，包括：改密前备份、备份失败不改密、密码恢复、手工验证密码、调试改密等；支持邮件、FTP、SFTP 等发送方式，改密后的密码可支持加密分段发送；支持对进行中任务实时停止。</p> <p>文件传输审计要求：支持保存 SSH 的 sz/rz 命令（zmodem）和 SFTP/FTP 传输的原始文件；</p> <p>内置根据运维人员生成各种维度的分析报表，维度包含运维次数、时长、运维时长、活动时长、会话大小、字符命令数、传输文件数、来源 IP 访问数、运维时间分布等。可分别从全局及平均值、最大值、最小值、单次运维、单个会话等角度提供；内置丰富的报表统计模板，可点击曲线图进行数据钻取分析，且支持 PDF、DOC、HTML 格式导出；</p> <p>系统自审：支持自身审计，包括但不限于：系统状态检测、登录日志、用</p>

	<p>户日志、资产日志、策略操作日志、审计日志、配置日志、维护日志、运维日志等。</p>
日志审计	<p>独立完成审计日志采集，不依赖于设备或系统自身的日志系统。</p> <p>支持预设置安全告警策略；支持告警数据阈值设置，超过阈值将产生告警。</p> <p>支持磁盘空间阈值告警，当磁盘使用率达到设定的阈值时可产生并外发告警。</p> <p>提供一键式故障排除功能。</p>
零信任（VPN接入）	<p>性能要求：最大并发用户数：1200；HTTP 每秒业务请求数量：20000TPS；业务转发时延≤25ms；HTTPS 加密吞吐量：5.6Gbps；最大 HTTP 并发连接数：10 万。</p> <p>提供用户组管理，可手工创建用户组并分配成员，支持组织机构通过上下拖移方式进行排序显示，支持通过停用组织方式，批量停用当前组织和下级组织所有用户。</p> <p>支持提供用户、组织、用户分组的统一管理功能，包括用户信息批量删除、锁定、停用、修改有效期，并可以用户导入、用户状态管理、用户同步等功能。</p> <p>提供本地用户账号密码安全机制，支持密码复杂度、密码错误超过阈值锁定，支持提供首次登录密码修改、密码定期修改、密码修改验证等功能。</p> <p>提供本地用户账号密码安全机制，支持密码复杂度、密码错误超过阈值锁定，支持提供首次登录密码修改、密码定期修改、密码修改验证等功能</p> <p>支持管理配置终端环境监控项，包括但不限于：网络信息、进程信息、软件安装信息、服务运行信息等。</p> <p>支持启用授信终端，只允许配置的授信终端才能访问控制器</p> <p>支持移动端操作系统版本、蓝牙开启、防病毒软件安装、互联网连接、Wi-Fi 热点开启等环境感知和采集，以实现基于移动终端安全状况的访问控制措施；</p> <p>支持用户行为分析，支持访问地址变更、非常用 IP、访问时间、IP 地址列</p>

	<p>表等用户行为数据采集，以实现基于用户行为状况的访问控制措施。</p> <p>支持配置应用账号与用户主账号的关联关系，支持将应用配置修改自动同步到零信任应用代理网关。</p> <p>系统权限管理模块采用角色授权模型，支持管理员、操作管理员、权限管理员、系统管理员、审计管理员、租户管理员的多种角色管理机制，区分菜单权限。</p>
代码审计	<p>依据 GB/T 39412-2020《信息安全技术代码安全审计规范》，信息系统开展软件代码审计，完成初测并提供初测报告，开发单位完成问题整改后对信息系统进行复测，确保信息系统的各项技术措施及管理手段能够满足标准要求。</p>
高危隐患和安全事件预警	<p>处理安全运维过程中政务云网络安全通告事件，发现安全问题及时通报用户，并指导用户进行相关修复工作，并提供整改建议。</p>
网络安全流量监测能力服务	<p>异常流量由安全运营中心研判后，监测结果快速通过邮件、短信、微信服务号及电话方式与用户进行沟通处置；监测结果纳入安全运营支撑系统中，参与脆弱性全生命周期的脆弱性管理，依据相应的运营脚本驱动风险处置过程。</p>
数据库权限管控系统	<p>依据 GB/T 37988-2019《信息安全技术 数据安全能力成熟度模型》，针对数据处理安全，对数据库使用人员相关数据库操作进行权限管控，包括数据库增删改查等相关动作，确保数据处理正当使用，完善数据处理环境。</p>
数据库审计	<p>依据《网络安全等级保护定级指南》要求，建立对应的数据库审计技术平台，完成对数据库具体操作的全量审计，管理者利用平台对数据库操作进行追踪溯源，同时定期导出审计报表。</p>
动态脱敏	<p>依据 GB/T 37988-2019《信息安全技术 数据安全能力成熟度模型》，针对数据处理安全，对数据进行脱敏处理，保障数据的安全性和平衡性。</p>
数据备份	<p>依据 GB/T 37988-2019《信息安全技术 数据安全能力成熟度模型》，针对数据存储安全，定期对重要数据进行备份，同时满足等保要求，定期对数据进行恢复演练。</p>

数据库运维及安全评估报告	针对数据库运行，通过人工加工具监测的方式，对数据库运行情况、数据库配置参数、数据库性能指标、数据库运行状态等进行监控，提供数据库运行情况以及安全评估报告和整改建议。
数据库入侵防护（云数据库防火墙）	利用数据库防火墙，对数据库 SQL 注入、漏洞等攻击行为进行实时阻断告警，定期导出防御日志。
攻防演练服务（包含红队（不少于 6 支红队，每队不少于 3 人）、紫队、演练方案、平台资源、人员协同、结果报告、演练复盘、加固改进建议报告等）	<p>（1）服务内容</p> <p>以协办的角色提供攻防演练组织服务，包括但不限于：演习组织协调、平台资源搭建、过程监控、技术指导、应急保障、演习成果报告汇总、演练复盘及安全整改加固报告输出等。通过攻防演练组织服务，提高参演单位安全威胁应对能力、攻击事件检测发现能力、事件分析研判能力和事件响应处置能力，提升参演单位的网络安全实战防护水平。</p> <p>（2）服务要求</p> <p>1) 须配合招标人成立攻防演练指挥部，组织协调红队队伍，并确保不少于 6 支红队，每队不少于 3 人；</p> <p>2) 须配合招标人制定攻防演练实施方案，确定演练攻击靶标、演练流程、演练场地、后勤保障措施及演练规则等；</p> <p>3) 须提供攻防演练平台资源，记录和展示双方攻防成果；至少提供一名技术专家支撑平台部署、应急和其他技术问题解决。</p>
重要活动时期安全保障服务：7*8 小时现场值守	<p>（1）服务内容</p> <p>重要节会活动期间，派遣一名安全专家提供现场 7*8 小时安全值守服务，根据既定岗位职责开展安全事件实时监测工作，加强重要时期网络安全威胁事件监控水平。</p> <p>（2）服务要求</p> <p>须提供 7*8 小时现场值守，按照采购人要求，记录安全设备监测信息，对告警信息进行预判，确认为安全事件的告警须第一时间上报。</p>
（资深专家，	（1）服务内容

<p>具有网络安全保障、攻防演练经验，负责监测预警、研判分析、攻击溯源等)</p>	<p>攻防演练或重要节会活动期间，派遣一名资深安全专家提供安全保障服务，通过对安全事件进行准确定位、研判控制、分析及处置，快速控制影响、减少损失，确保特殊时期系统安全稳定地运行。</p> <p>(2) 服务要求</p> <p>1) 须对受事件的影响目标系统进行快速检测，并对事件进行分析研判，在明确事件等级和危害程度后，制定事件抑制措施，协助监测人员对事件进行抑制，降低事件影响；</p> <p>2) 须采取必要的措施对网络攻击事件进行追踪溯源。溯源方式不限于：社交 id 溯源、钓鱼邮件反钓鱼、攻击地址反查等。</p>
<p>渗透服务</p>	<p>针对系统采用完全模拟入侵者可能采用的攻击技术和漏洞发现技术，利用专家经验对用户系统进行非破坏性质的模拟攻击，发现系统的最脆弱的环节和弱点等安全问题，为进一步加固信息系统提供了依据，并出具渗透测试报告。</p>

9) 机柜租赁服务

指标项	规格要求
<p>技术要求</p>	<p>提供独立综合机房，按需提供机柜空间，用以放置服务器、交换机、磁盘阵列、网络设备等。</p>
	<p>电力供应保障：机房引入 2 路市电，配置柴油发电机组，市电油机可自动切换；机房具备单独电力室，配备不低于 400KVA 的 1+1 或 2N 的 UPS。</p>
	<p>环境保障：机房内配置机房精密空调，可确保设备运行对环境温湿度的要求；配备完善的气体消防系统、防湿防水系统。</p>
	<p>具备机房动环监测及报警系统、门禁系统；机房环境符合等保三级相关要求。</p>
<p>管理要求</p>	<p>运维值班：提供 7*24 小时机房运维值班及技术支持，对相关设备进行巡检、维护和监控（包括防静电、防火、机房内温湿度，对机器重启、监控网络是否正常），保障设备正常运行。</p>
	<p>日常管理：指派专人负责对机房人员及设备进出登记管理（人员与设备进</p>

	出需经用户方审批同意），记录设备使用单位、人员及承载业务系统情况，建立相关台账；每季度提供运维报告。
	机柜使用率（设备占用 U 位除以机柜总 U 位，设备之间距小于或等于 2U 算占用）：每季度一次与托管设备单位确认更新在用设备及承载业务系统运行情况，及时下架未使用设备。

4. 衢州市政务云服务（非 XC 部分）技术要求

1) 基础云资源服务

a. 云主机

指标项	规格要求
服务标准	根据用户的需求动态地创建和分配计算资源与存储资源。
服务特性	云主机创建。创建后，云主机已包含有操作系统，可立即使用，从创建到启动在 5 分钟以内。
	云服务器提供快照制作，快照回滚，自定义 image，动态升级，可以为每块磁盘创建快照。
	支持虚拟机故障切换，在线迁移；支持宿主机宕机迁移。
	主机之间网络访问逻辑隔离，支持创建和管理安全组；提供安全组的创建、修改、删除以及批量删除等功能。
	需提供丰富的 API 接口，包括资源的创建，删除，修改，查询，启动等操作。
	云服务器工作节点采用分布式高可用架构，保障云服务器的高可用。
	支持资源开通时指定 IP 地址。
服务能力	支持故障切换，动态迁移，多数据备份等。

b. GPU云主机

指标项	规格要求
基本功能	支持 GPU 直通，从容应对高实时、高并发的海量计算场景，可以将一块 GPU 卡直通给一个虚拟机，支持主流 GPU 的直通。
其他	继承云主机功能及安全特性。

c. 块存储

指标项	规格要求
功能要求	支持在线扩展容量，扩容期间无需关闭虚拟机，无需卸载云盘；系统盘在线扩容不停业务。
	支持磁盘的创建、删除、卸载、扩容、挂载、查询、初始化等功能。
总体要求	为云主机提供的低时延、持久性、高可靠性的数据块级存储设备。
安全性	支持分布式 EC 或三副本数据冗余保护，三副本模式下，数据三副本支持分布在 3 个机柜或 3 对接入交换机上。

d. 对象存储

指标项	规格要求
服务标准	提供基于三副本或 EC 校验模式的数据多重冗余备份，保证数据安全。
服务特性	提供 key-value 键值对形式的对象存储服务。
	具备多用户隔离机制。
	支持大文件的分片并发上传和下载，支持断点续传。
	提供日志记录功能，方便追查访问来源以及进行多维度的统计分析。
	提供服务端数据加密。
	支持对象简单上传/表单上传/下载/下载到本地文件/删除/批量删除生命周期管理。
安全访问	支持 Bucket 级别的 ACL。

e. 负载均衡

指标项	规格要求
服务要求	支持四层负载均衡和七层负载均衡； 支持集群高可用架构，支持动态扩展。
服务特性	协议支持：提供四层（TCP 协议和 UDP 协议）和七层（HTTP 和 HTTPS 协议）的负载均衡服务。
	应提供多种转发规则，满足不同业务场景的要求：域名、url 转发。
	健康检查：提供后端 ECS 实例的健康检查。负载均衡服务会自动屏蔽异常

	状态的 ECS 实例，待该 ECS 实例恢复正常后自动解除屏蔽。
	调度算法：支持轮询、最小连接数两种调度算法： ∞轮询：按照访问次数依次将外部请求依序分发到后端 ECS 实例上。 ∞最小连接数：连接数越小的后端服务器被轮询到的次数（概率）也越高。
	访问控制：支持白名单访问控制。通过添加负载均衡监听的访问白名单，仅允许特定 IP 访问负载均衡服务。
可靠性	管理节点采用全冗余架构。

f. 云数据库（Mysql\SQLServer）

指标项	指标要求
基本功能/性能	基于高效的调度、备份、HA 控制、在线迁移以及监控系统，为用户提供专业的云数据库服务。
	提供数据库自主诊断、慢查询分析，提供全面的健康状态以使用户自动化运维。
	支持 SQL Server、MySQL 等主流关系型数据库。
	可提供稳定可靠、可弹性伸缩的在线关系型数据库服务。
	提供完善的备份、恢复机制，支持手工备份和自动备份，支持物理备份和逻辑备份、逻辑备份支持库级备份，并支持恢复到指定时间点。
	支持业务无中断在线方式升级数据库规格及存储空间。
扩展功能	按需开通，即开即用，为用户提供方便的 Web 管理界面。
	为了满足大量读请求的应用场景，需要支持原生只读实例和读写分离功能，可支持不少于 5 个只读实例，自动实现读写分离以及读节点间的负载均衡。
	支持对 MySQL 可视化日志管理，包括慢日志、错误日志、数据库主备切换日志等。
安全性	具备完善的安全防护措施，支持白名单设置、SQL 审计等功能。
	云服务端提供加密用户身份验证，提供不同的访问权限控制。
兼容性/开放性	支持主流的数据库引擎，并提供完善的 OpenAPI 供外部调用。

可靠性	采用全冗余架构，无单点故障。支持单 AZ 主备高可用和 3 节点架构，及同城 2AZ 主备高可用和 3AZ 3 节点高可用架构。
-----	------------------------------------------------------------------

g. 数据库MongoDB

指标项	具体要求
功能要求	兼容多个 MongoDB 版本，支持通配符索引，支持 JSON 数据模型，二级索引能力。
	提供多种规格的 MongoDB 实例，支持实例的创建、重启、管理、变配、释放等操作，支持实例的网络隔离。
	支持副本、分片集群架构，支持多种规格，支持集群角色主备自动和手动切换。
	支持空间分析功能，包括库表空间概况，空间变化趋势，异常列表和表空间信息，可及时发现数据库中空间的异常情况。
总体要求	可提供稳定可靠，完全兼容 MongoDB，支持多节点高可用的文档型数据库服务。
可靠性	支持对数据文件的物理备份和逻辑备份方式，支持自动和手动备份，支持设置自动备份策略，支持备份的回滚恢复、恢复到新实例和备份文件下载，支持按照备份集和时间点进行数据恢复。
	支持对 cpu、内存、iops、磁盘空间、网络流量、连接数、主备延迟等指标进行监控。
安全性	支持 IP 白名单设置，提供灵活的安全访问管理能力。
	支持 TDE 存储加密和 SSL 传输加密等安全加密能力，存储加密支持用户自定义密钥（BYOK）。
	支持开启、关闭、查看、导出审计日志，支持查看用户，客户端 IP，执行语句，消耗时间等审计信息，还可以通过数据库，关键词、时间范围等信息进行日志筛选。

2) 大数据服务

a. 大数据服务

指标项	规格要求	
功能指标	节点调度	超大规模节点调度能力，具备单集群 30000 节点以上调度能力。为保证大数据集群具有高可扩展性。
	集群规模	采用分布式计算框架提供大规模数据存储与计算，可按需扩容。
功能要求	功能特性	支持 MapReduce 类型的分布式计算任务，支持 DAG 模式的作业处理方式。
	功能特性	支持多种计算框架如 SQL、MapReduce、Spark、Graph。
	功能特性	支持原生 Apache Spark 编程接口，用户可以使用 Spark 接口进行编程处理存储在大数据计算服务中的数据。
	功能特性	提供完整 RESTful API 的方式提供离线数据处理服务，提供 JAVA SDK, Python SDK, 等编程接口，支持 JDBC 接口等系列用户开发工具和接口。
	功能特性	提供离线任务管理、监控告警的功能。

b. 大数据开发治理平台

指标项	规格要求
基础功能	为数据仓库/数据湖/湖仓一体等解决方案提供统一的全链路大数据开发治理平台。
数据集成	支持多数据源之间的数据接入和同步。
数据开发	通过 SQL 编辑器实现代码输入，包含关键字、函数、表、字段等信息；支持错误语法实时提示。
运维中心	支持调度系统诊断，完善调度系统作业的性能和稳定性。
数据质量	支持数据质量校验规则与调度系统结合，数据产出后立即触发任务调度，若配置的强规则校验失败，则将任务状态置为失败，避免脏数据对下游作业产生污染。
数据服务	服务编排：提供拖拽式、可视化的服务编排能力，支持用户按照业务逻辑，以串行、并行和分支等结构编排多个 API 及函数服务为工作流。

数据保护伞	<p>分级管理：自定义数据安全等级。</p> <p>数据脱敏：包含有敏感信息的数据库，对敏感信息进行动态遮蔽。</p>
迁移助手	支持新建导出任务。

3) 其他服务

a. 云产品备份

云产品	指标项	规格要求
ECS 云主机	基础功能	支持用户通过快照对云主机的数据进行备份。
	指标要求	支持用户通过快照对云主机的数据进行备份，通过快照进行云服务器的数据恢复，可以为每块磁盘创建 64 个快照。
RDS 数据库	功能要求	支持至少五种主流数据库类型备份：包括但不限于 MySQL、PostgreSQL、MongoDB、Redis、Oracle。
		支持对公网 IP 自建、虚拟机自建、本地机房自建、专有云多种位置形态创建的数据库实例备份恢复。
		支持整个实例、多个数据库、单个数据库、多张表、单表、视图、存储过程、触发器、函数备份。
		支持备份频率、周期、开始时间、并行线程数等备份计划配置。
		支持全量和增量备份保留时长配置到期自动删除。
		支持计划外手动发起全量备份。
		支持恢复时间点配置。
		支持恢复目标库新建实例或者使用已有实例。
		支持备份到三方存储池，包括文件存储、对象存储。
		支持批量自动接入新增数据源实例。
总体要求	总体要求	支持相同的数据库类型和相同的备份类型的批量配置备份计划。
		数据库备份服务是为数据库提供连续数据保护、低成本的备份服务，它可以为多种环境的数据提供强有力的保护，

		包括企业数据中心、其他云厂商及公有云，数据库备份拥有一套完整的数据备份和数据恢复解决方案，具备实时增量备份以及精确到秒级的数据恢复能力。
	安全性	支持 AES256 加密技术保护备份数据存储安全。

b. 分布式应用

指标项	规格要求
服务标准	提供应用开发、部署、监控、运维等全栈式解决方案，支持Dubbo或SpringCloud等微服务运行环境。
服务特性	涵盖了应用生命周期管理、运维管控等众多功能。
	弹性伸缩：弹性伸缩能够感知应用内各个实例的状态，并根据状态动态实现应用扩容、缩容。在保证服务质量的同时，提升应用的可用率。
	限流降级：限流降级用于解决后端核心服务因压力过大造成系统反应过慢或者崩溃问题。
	健康检查：健康检查对容器与应用进行定时检查和汇报，然后将结果上报到控制台，可以了解集群环境下整个应用的运行状态，排查和定位问题。
	灰度发布：灰度发布包括对单个应用的灰度发布和全链路灰度发布。通过灰度发布实现应用新、旧版本的平滑过渡。
服务能力	生命周期管理操作。 生命周期管理包括创建、部署、扩容、缩容、停止、删除等。因部署的集群类型不同，生命周期管理操作有些差异。
	应用监控，在应用托管到分布式应用后，可以对应用进行监控。包括基础监控、服务监控、日志和通知报警。

c. 主机托管

指标项	规格要求
技术要求	提供独立综合机房，按需提供机柜空间，用以放置服务器、交换机、磁盘阵列、网络设备等。
	电力供应保障：机房引入 2 路市电，配置柴油发电机组，市电油机可自动

	切换；机房具备单独电力室，配备不低于 400KVA 的 1+1 或 2N 的 UPS。
	环境保障：机房内配置机房精密空调，可确保设备运行对环境温湿度的要求；配备完善的气体消防系统、防湿防水系统。
	具备机房动环监测及报警系统、门禁系统；机房环境符合等保三级相关要求。
管理要求	运维值班：提供 7*24 小时机房运维值班及技术支持，对相关设备进行巡检、维护和监控（包括防静电、防火、机房内温湿度，对机器重启、监控网络是否正常），保障设备正常运行。
	日常管理：指派专人负责对机房人员及设备进出登记管理（人员与设备进出需经用户方审批同意），记录设备使用单位、人员及承载业务系统情况，建立相关台账；每季度提供运维报告。
	机柜使用率（设备占用 U 位除以机柜总 U 位，设备之间距小于或等于 2U 算占用）：每季度一次与托管设备单位确认更新在用设备及承载业务系统运行情况，及时下架未使用设备。

d. 视频云存储

指标项	规格要求
功能要求	支持视音频、图片、直接写入，支持视频高速预览、回放、下载，支持云内容灾备份，支持一体化运维，支持 GB/T28181-2011、Onvif、RTSP、H265、SVAC 等标准视频协议。
	支持图片流直存，抓拍图片无需经过任何转发服务器/虚拟机即可实现前端数据直接存储至云存储系统；支持设置资源池自动分流策略，策略包含按图片大小、图片类型。支持将同一点位产生的多种不同大小、不同类型的图片数据按策略自动分池存储到不同存储资源池中。
	系统支持手动、自动对智能事件关联的多个录像片段设置录像标签。支持标签与其关联的录像片段同生命周期管理；支持通过按标签内容查询、回放、下载录像片段数据；支持对标签关联的录像片段进行锁定、备份。
	支持图形化页面对图片数据进行处理，包括图片预览、压缩、裁剪、旋转、

	缩放、格式转换、马赛克、归一化及打文字水印，并支持通过图形化页面下载处理成功的图片数据。
总体要求	提供低时延、持久性、高可靠性的数据块级存储设备。
安全性	基于纠删码的容错网络 RAID 技术，保证设备级数据安全。
	极速智能恢复技术，可快速修复用户数据，不影响用户和数据的可可用性。
	具有国家密码管理局商用密码检测中心出具“云存储平台系统密码安全功能和性能检测报告”。

4) 安全服务

提供网络安全（漏洞扫描、云堡垒机、日志审计、WEB 防火墙等）、渗透服务、应用安全（代码审计、主机安全防护等）、数据安全等服务（数据库权限管控、数据库审计、静态脱敏等），具体如下表：

安全产品	技术要求
漏洞扫描	<p>支持对各种网络主机、操作系统、网络设备（如交换机、路由器、防火墙等）、常用软件以及应用系统的识别和漏洞扫描；</p> <p>用户可自定义扫描端口范围、端口扫描策略等扫描选项；</p> <p>支持对各种网络主机、操作系统、网络设备（如交换机、路由器、防火墙等）、常用软件以及应用系统的识别和漏洞扫描；</p> <p>支持手动创建资产也可以批量导入资产，在资产管理页面可直接对单个资产或批量资产下发扫描任务；</p> <p>支持自定义扫描策略模板，可以将自定义策略模板导出备份，也可以导入备份的策略模板，能够对策略模板进行编辑、另存为新的模板；</p> <p>支持导出的报告类型≥5 种，包括 HTML、WORD、PDF、EXCEL、XML 报告格式。</p>
主机安全防护	<p>支持防端口扫描，锁定恶意的端口扫描，并记录告警；</p> <p>支持病毒库、Windows 补丁库的离线升级及在线升级；支持管理平台、终端软件安装包、终端软件更新包、系统漏洞库、弱口令库的离线升级。</p> <p>支持按照防护类别筛选日志，包括：高级威胁、系统防护、网络防护、We</p>

	<p>b 应用防护。</p>
<p>WEB 应用防火 墙</p>	<p>性能要求：HTTP 应用层吞吐量：9537.182Mbps，HTTP 最大并发数：279.999 万，HTTP 最大新建：6.803 万/秒。</p> <p>产品符合自主可控关键核心技术要求。</p> <p>支持透明串接、反向代理、旁路镜像等多种部署模式部署，支持链路聚合。</p> <p>支持 ipv4/ipv6 双协议栈。</p> <p>支持源地址识别，部署在 SSL 网关后面，能够解析到真实的访问者 IP，并能对真实的 IP 进行防护和阻断。</p> <p>支持对跨站脚本（XSS）和注入式攻击（包括 SQL 注入、命令注入、代码注入、文件注入、LDAP 注入、SSI 注入等）的检测防护（提供功能截图）；</p> <p>内置 Webshe11 检测规则，可以对上传的文件内容进行检查，防止恶意 Web she11 文件上传，对已经上传的 Webshe11 发起请求的行为进行拦截阻断。</p> <p>能够检测防止服务器导致的信息泄露行为，包括：目录信息泄露、服务器信息泄露、数据库信息泄露、源代码泄露等信息泄露行为。</p> <p>内置安全规则可有效识别 Acunetix、nessus、WebScan、Webdump、AppScan 等扫描器的扫描行为。</p> <p>支持对 HTTP 请求中 URI、HOST、参数、参数名、请求头、Cookie、版本号、方法和请求体及 HTTP 响应的响应体等条件进行自定义正则。</p> <p>支持阻断、重定向、智能加黑名单、丢弃、告警、仅检测等动作。不同的防护规则，可以选择不同的防护动作及返回码，也可针对不同规则设置专属 URL 白名单。</p> <p>具有机器学习安全引擎，可以对用户 web 业务系统建立安全的访问模型，学习的内容包括 URL 地址、URL 请求参数等信息。</p> <p>WAF 支持与 APT 产品联动实现对未知威胁的感知拦截。</p> <p>能详细记录攻击事件的 HTTP 请求头信息，含请求的 URL、UserAgent、POST 内容，cookie 等所有的请求头内容支持报表导出为 Word、pdf、html 等</p>

	<p>多种格式。</p> <p>规则库支持手工、在线升级两种方式，在线升级可支持规则定时检查新版本和在线更新，确保 WAF 能够针对新型的、突发型的 Web 攻击进行防护。</p>
云堡垒机	<p>支持用户多角色划分功能，如系统管理员、部门管理员、运维员、审计管理员、密码管理员等，对各类角色需要进行细粒度的权限管理。支持自定义用户权限；</p> <p>支持完善的自动改密安全保护机制，包括：改密前备份、备份失败不改密、密码恢复、手工验证密码、调试改密等；支持邮件、FTP、SFTP 等发送方式，改密后的密码可支持加密分段发送；支持对进行中任务实时停止；</p> <p>文件传输审计要求：支持保存 SSH 的 sz/rz 命令（zmodem）和 SFTP/FTP 传输的原始文件；</p> <p>内置根据运维人员生成各种维度的分析报表，维度包含运维次数、时长、运维时长、活动时长、会话大小、字符命令数、传输文件数、来源 IP 访问数、运维时间分布等。可分别从全局及平均值、最大值、最小值、单次运维、单个会话等角度提供；内置丰富的报表统计模板，可点击曲线图进行数据钻取分析，且支持 PDF、DOC、HTML 格式导出；</p> <p>系统自审：支持自身审计，包括但不限于：系统状态检测、登录日志、用户日志、资产日志、策略操作日志、审计日志、配置日志、维护日志、运维日志等。</p>
日志审计	<p>可对日志进行细粒度解析，解析后的日志根据具体日志包含但不限于：日期、发生时间、接收时间、设备类型、日志类型、日志来源、威胁值、源地址、目的地址、事件类型、时间范围、操作主体、操作对象、行为方式、技术动作、技术效果、攻击类型、特征类型、协议。</p> <p>支持预设置安全告警策略；支持告警数据阈值设置，超过阈值将产生告警。提供一键式故障排除功能。</p>
零信任（VPN 接入）	<p>性能要求：最大并发用户数：1200；HTTP 每秒业务请求数量：20000TPS；业务转发时延\leq25ms；HTTPS 加密吞吐量：5.6Gbps；最大 HTTP 并发连</p>

	<p>接数：10 万。</p> <p>提供用户组管理，可手工创建用户组并分配成员，支持组织机构通过上下拖移方式进行排序显示，支持通过停用组织方式，批量停用当前组织和下级组织所有用户。</p> <p>支持提供用户、组织、用户分组的统一管理功能，包括用户信息批量删除、锁定、停用、修改有效期，并可以用户导入、用户状态管理、用户同步等功能。</p> <p>提供本地用户账号密码安全机制，支持密码复杂度、密码错误超过阈值锁定，支持提供首次登录密码修改、密码定期修改、密码修改验证等功能。</p> <p>提供本地用户账号密码安全机制，支持密码复杂度、密码错误超过阈值锁定，支持提供首次登录密码修改、密码定期修改、密码修改验证等功能。</p> <p>支持管理配置终端环境监控项，包括但不限于：网络信息、进程信息、软件安装信息、服务运行信息等。</p> <p>支持启用授信终端，只允许配置的授信终端才能访问控制器。</p> <p>支持移动端操作系统版本、蓝牙开启、防病毒软件安装、互联网连接、Wi-Fi 热点开启等环境感知和采集，以实现基于移动终端安全状况的访问控制措施；</p> <p>支持用户行为分析，支持访问地址变更、非常用 IP、访问时间、IP 地址列表等用户行为数据采集，以实现基于用户行为状况的访问控制措施。</p> <p>支持配置应用账号与用户主账号的关联关系，支持将应用配置修改自动同步到零信任应用代理网关。</p> <p>系统权限管理模块采用角色授权模型（RBAC），支持管理员、操作管理员、权限管理员、系统管理员、审计管理员、租户管理员的多种角色管理机制，区分菜单权限。</p>
<p>渗透服务</p>	<p>针对系统采用完全模拟入侵者可能采用的攻击技术和漏洞发现技术，利用专家经验对用户系统进行非破坏性质的模拟攻击，发现系统的最脆弱的环节和弱点等安全问题，为进一步加固信息系统提供了依据，并出具渗透测</p>

	试报告。
代码审计	依据 GB/T 39412-2020《信息安全技术代码安全审计规范》，信息系统开展软件代码审计，完成初测并提供初测报告，开发单位完成问题整改后对信息系统进行复测，确保信息系统的各项技术措施及管理手段能够满足标准要求。
高危隐患和安全事件预警	处理安全运维过程中大数据政务云网络安全通告事件，发现安全问题及时通报用户，并指导用户进行相关修复工作，并提供整改建议。
网络安全流量监测能力服务	异常流量由安全运营中心研判后，监测结果快速通过邮件、短信、微信服务号及电话方式与用户进行沟通处置；监测结果纳入安全运营支撑系统中，参与脆弱性全生命周期的脆弱性管理，依据相应的运营脚本驱动风险处置过程。
数据库权限管控系统	依据 GB/T 37988-2019《信息安全技术 数据安全能力成熟度模型》，针对数据处理安全，对数据库使用人员相关数据库操作进行权限管控，包括数据库增删改查等相关动作，确保数据处理正常使用，完善数据处理环境。
数据库审计	依据《网络安全等级保护定级指南》要求，建立对应的数据库审计技术平台，完成对数据库具体操作的全量审计，管理者利用平台对数据库操作进行追踪溯源，同时定期导出审计报表。
静态脱敏	依据 GB/T 37988-2019《信息安全技术 数据安全能力成熟度模型》，针对数据处理安全，对数据进行脱敏处理，保障数据的安全性和平衡性。
数据备份	依据 GB/T 37988-2019《信息安全技术 数据安全能力成熟度模型》，针对数据存储安全，定期对重要数据进行备份，同时满足等保要求，定期对数据进行恢复演练。
数据库监控平台服务	利用监控平台，对数据库相关运行情况、数据库运行状态等进行实时监控。
数据库运维及安全评估报告	针对数据库运行，通过人工加工具监测的方式，对数据库运行情况、数据库配置参数、数据库性能指标、数据库运行状态等进行监控，提供数据库运行情况以及安全评估报告和整改建议。

数据库入侵防护（云数据库防火墙）	利用数据库防火墙，对数据库 SQL 注入、漏洞等攻击行为进行实时阻断告警，定期导出防御日志。
------------------	------------------------------------------------

二、服务清单及限价

（一）xc 云产品服务

主要内容为衢州市电子政务信息化系统提供所需 xc 计算资源云计算服务。主要内容包含租赁服务主要包括如下基础云服务、中间件服务、安全服务、大数据服务等服务：

产品类别	产品子类	服务名称	计费方式	单位	最高限价（元/月）
基础服务	云主机服务	云主机（不含操作系统）	根据核数，按月计费（v CPU 主频）=2.2GHz）	core	49.7
			根据内存，按月计费	GB	29.85
	快照	ECS 快照服务	根据存储容量，按月计费	GB	0.2
自主可控关键技术服务	自主可控关键技术软件	国产 WEB 中间件软件	按照配置规格计费（套），按月计费	套	830
		国产操作系统	按照配置规格计费（套），按月计费	套	80
		国产数据库软件	按照配置规格计费（套），按月计费	套	2000
存储服务	块存储服务	高效云盘	根据存储容量，按月计费	GB	0.63
		SSD 云盘	根据存储容量，按月计费	GB	1
		数据库存储	根据存储容量，按月计费	GB	1.03
	对象存储服务	对象存储	根据存储容量，按月计费	GB	0.2
	视频云存储	视频云存储	根据存储容量，按月计费	GB	0.042
	数据库存储备份服务	数据库备份存储	根据备份存储容量，按月计费	GB	0.83
	日志服务	日志服务	根据存储容量，按月计费	GB	0.33
网络服务	负载均衡	负载均衡	根据实例个数，按月计费	1 实例	48
	VPC	VPC	根据实例个数，按月计费	1 实例	25.37
	公网 IP	公网 IP	按 1Mbps/1 个公网 IP 计费	个	37
	公网带宽	公网带宽	公网带宽每 Mbps 价格（ipv6），按月计费。若使用政务外网带宽则不收费。	Mbps	14.17

产品类别	产品子类	服务名称	计费方式	单位	最高限价(元/月)
	云网络服务	NAT 网关	根据实例类型数量+公网 IP 数, 按月计费	1 实例	29.5
				性能共享型	13
		高速通道	根据跨专有网络互通策略数量, 按月计费	每策略	27
		DNS 服务	根据 Zone 数量+每个 ZONE 的请求次数(以每万次为 1 个规格递增), 按月计费	计费项 1: Zone 数量	2.07
				计费项 2: 每个 ZONE 的请求次数	0.8
云数据库服务	云数据库-类型 I (兼容 MySQL、Oracle)	云数据库	根据核数, 按月计费	core	210
			根据内存, 按月计费	GB	140
	云数据库-类型 II (兼容 MySQL)	通用型	根据核数, 按月计费	core	45
			根据内存, 按月计费	GB	35
		独享型	根据核数, 按月计费	core	59.15
			根据内存, 按月计费	GB	46.15
	云数据库-类型 III (兼容标准 SQL)	云数据库	根据核数, 按月计费	core	233
			根据内存, 按月计费	GB	105
	分布式关系型数据库	分布式关系型数据库	根据核数和内存容量, 按月计费	核数: core	101
				内存容量: GB	68
应用服务	应用实时监控服务	应用实时监控服务	根据应用监控资源包+前端页面监控资源包, 按月计费	应用监控资源包: 1 个 Agent	198
	消息中间件	消息队列	根据实例 (Topic 数量+消息发送 TPS+消息订阅 TPS) 按月计费	Topic 资源包: 1 个	45
				消息发送基础包: 1TPS	2
				消息发送扩展包: 1TPS	1.9
				消息订阅基础包: 1TPS	1.9
				消息订阅扩展包: 1TPS	1.9
	容器服务	容器服务	根据 ECS 节点数量(不包含资源费用), 按月计费	ECS 节点数量	170

产品类别	产品子类	服务名称	计费方式	单位	最高限价 (元/月)
	API 网关服务	API 网关	根据配置规格, 按月计费	每 1RPS	0.9
大数据服务	大数据服务	大数据计算服务	根据实例开通的 CU 数+ 存储容量 (100G 起步)+ 增强软件包 (非必选), 按月计费	实例开通 CU 数: CU	118
				存储容量: GB	0.64
			大数据多维分析服务(警 务节点服务)	实例开通 CU 数: CU	118
				存储容量: GB, SSD	1
			大数据消息缓存服务(警 务节点服务)	实例开通 CU 数: CU	118
				存储容量: GB, SSD	1
	实时计算服务	根据实例开通的 CU 数, 按月计费	实例 CU 数: CU	129	
	大数据搜索 与分析	搜索服务	根据数据节点配置单价 及数量+专有主节点配置 单价及数量+协调节点配 置单价及数量+存储类型 及空间及数量, 按月计费	数据节点 CPU: 每核	41.16
				数据节点内存: 每 G	25.4
				专有主节点 CP U: 每核	90
				专有主节点内 存: 每 G	62
				协调节点 CPU: 每核	25
				协调节点内存: 每 G	17
存储计费: 高效 云盘 (GB)				0.63	
数据治理与 分析	大数据开发治理 平台	标准版	根据租户开通 的版本按月收 费, 按套计费	5000	
容灾 备份 服务	异地备份服 务	异地备份存储	根据备份存储容量, 按月 计费	GB	0.15
		异地备份实例类 型	根据备份的实例类型及 数量, 按月计费	文件备份软件 服务 (计算服 务)	39

产品类别	产品子类	服务名称	计费方式	单位	最高限价(元/月)	
				应用备份软件服务(数据库、大数据服务)	153	
传输服务	传输专网	云平台之间容灾用 10G 专线(裸光纤)	根据条数, 按年计费	年/条	59200	
安全服务	基础版	网络安全	漏洞扫描	根据云主机数量, 按月计费	个	70
		主机安全防护	根据云主机数量, 按月计费	个	64	
		云堡垒机	根据云主机数量, 按月计费	个	30	
		日志审计	根据日志源, 按月计费	日志源	77.5	
		Web 应用防火墙	根据子域名/IP 数量, 按月计费	子域名/IP	200	
		零信任(VPN 接入)	根据账户数量, 按月计费	账户	35	
	应用安全	代码审计	根据系统数量, 按次计费	套	6000	
	高危隐患和安全事件预警	根据系统数量, 按月计费	套	445.5		
	网络安全流量监测能力服务	根据系统数量, 按月计费	套	445.5		
	数据安全	数据库权限管控系统	根据数据库实例, 按月计费	1 实例	1195	
	数据库审计	根据数据库实例, 按月计费	1 实例	455		
	动态脱敏	根据数据库实例, 按月计费	1 实例	672		
	数据备份	1/GB, 按月计费	1/GB	0.42		
	数据库运维及安全评估报告	每月巡检报告, 1 次	1 次	600		
	数据库入侵防护(云数据库防火墙)	根据套数, 按月计费	1 实例	840		
	选配包	攻防演练	攻防演练服务(包含红队(不少于 6 支红队, 每队不少于 3 人)、紫队、演练方案、平台资源、人员协同、结果报告、演练复盘、加固改进建议)	按次计费	1 次	195000

产品类别	产品子类	服务名称	计费方式	单位	最高限价 (元/月)
		报告等)			
		重要活动时期安全保障服务：7*8小时现场值守。 (资深专家，具有网络安全保障、攻防演练经验，负责监测预警、研判分析、攻击溯源等)	按每人/天计费	1人/天	2380
	渗透服务	渗透测试服务是模拟黑客攻击的方式，对业务系统的安全漏洞、安全隐患进行全面检测的安全服务。服务的最终目标是查找业务系统的安全漏洞、评估业务系统的安全状态，并提供相应的漏洞修复建议。	根据系统数量，按次计费	套	7800
专业人员服务	资深专业人员驻场服务	资深网络和数据安全工程师具备深厚的技术背景和安全意识，能够持续跟踪和研究网络安全领域的最新动态和趋势，负责设计、开发和维护网络和数据安全系统，以确保组织的信息资产和数据安全。	1人/月	1人	16300
	专业人员驻场服务	负责确保网络和数据安全的专业人员，涉及设计、实施和维护网络安全策略、安全架构以及安全系统，以预防、检测和应对网络安全威胁和数据泄露事件。	1人/月	1人	12800

产品类别	产品子类	服务名称	计费方式	单位	最高限价(元/月)
机柜托管	机柜服务	机柜租赁及服务器托管	机柜U数, 按月计费	1U/月	200

(二) 非xc云产品服务

主要为衢州市电子政务信息化系统提供所需非xc计算资源云计算服务。主要内容包含租赁服务主要包括如下基础云服务、中间件服务、安全服务、大数据服务等服务。

产品类别	产品子类	服务名称	计费方式	单位	最高限价(元/月)
基础服务	云主机服务	云主机(含符合要求的操作系统)	根据核数, 按月计费(vCPU主频≥2.2GHz)	core	36
			根据内存, 按月计费	GB	21.6
		GPU服务器	14核56G, 1×NVIDIA T4	1实例	1976
			28核112G, 2×NVIDIA T4	1实例	3290
			40核160G, 2×NVIDIA T4	1实例	4308
	块存储服务	高效云盘	根据存储容量, 按月计费	GB	0.35
		SSD云盘	根据存储容量, 按月计费	GB	0.65
		数据库存储	根据存储容量, 按月计费	GB	0.7
	对象存储服务	对象存储	根据存储容量, 按月计费	GB	0.15
	弹性IP	EIP	根据实例个数, 按月计费	1实例	30
	负载均衡	负载均衡	根据实例个数, 按月计费	1实例	40
	云数据库服务	RDS	通用型-MySQL	根据核数, 按月计费	core
根据内存, 按月计费				GB	40
独占型-MySQL			根据核数, 按月计费	core	75
			根据内存, 按月计费	GB	52
RDS		MS SQL	根据核数, 按月计费	core	66.4
			根据内存, 按月计费	GB	45.86
MongoDB	MongoDB	根据核数, 按月计费	core	99.8	
		根据内存, 按月计费	GB	68.8	
大数据服务	大数据服务	大数据计算服务	根据实例开通的CU数+存储容量(500G起步)+增强软件包(非必选), 按月计费	实例开通CU数: CU	100
			存储容量: GB	0.25	
	大数据开发治理平台	标准版	根据租户开通的版本按月收费, 按套计费	租户	5000

产品类别	产品子类	服务名称	计费方式	单位	最高限价(元/月)
其他服务	云产品备份服务	ECS/RDS 快照服务	ECS/RDS 快照服务	TB	200
	分布式应用服务	EDas 企业版	铂金版 (0-50) 实例	EDAS 租户	43000
	主机托管	主机托管	根据 U 数, 按月计费	1U	200
安全服务	网络安全	漏洞扫描	根据云主机数量, 按月计费	个	70
		云堡垒机	根据云主机数量, 按月计费	云主机	30
		日志审计	根据日志源, 按月计费	日志源	77
		态势感知	根据受保护的云主机个数按月计算, 默认按云主机一起开通	1 实例	48.1
		安骑士	根据受保护的云主机个数按月计算, 默认按云主机一起开通	1 实例	55.1
		Web 应用防火墙	根据子域名数量, 按月计费	子域名	200
		零信任 (VPN 接入)	根据账户数量, 按月计费	账户	35
	渗透服务	渗透服务	根据系统数量, 按次计费	套	7850
	应用安全	代码审计	根据系统数量, 按次计费	套	6000
		主机安全防护	根据云主机数量, 按月计费	个	60.8
		高危隐患和安全事件预警	根据系统数量, 按月计费	套	445.5
		网络安全流量监测能力服务	根据系统数量, 按月计费	套	445.5
	数据安全	数据库权限管控系统	根据数据库实例, 按月计费	1 实例	1195
		数据库审计	根据数据库实例, 按月计费	1 实例	455
		静态脱敏	1/GB, 按月计费	1/GB	7.87
		数据备份	1/GB, 按月计费	1/GB	0.4
		数据库监控平台服务	1 实例, 按月计费	1 实例	1000
数据库运维及安全评估报告		每月巡检报告, 1 次	1 次	600	
数据库入侵防护 (云数据库防火		根据数据库实例, 按月计费	1 实例	840	

产品类别	产品子类	服务名称	计费方式	单位	最高限价(元/月)
		墙)			

三、商务要求

(一) 服务期限

服务期 36 个月（自采购人组织服务能力验证通过后起计，最迟不晚于 2024 年 12 月 31 日）。

(二) 政务云平台服务等级协议（SLA）指标

产品分类	服务项目	可用性目标
计算服务	云服务器	单个实例 $\geq 99.95\%$ ，不可用时间须 ≤ 21.9 分钟/月
	GPU 云服务器	单个实例 $\geq 99.95\%$ ，不可用时间须 ≤ 21.9 分钟/月
存储服务	对象存储	单个实例 $\geq 99.95\%$ ，不可用时间须 ≤ 21.9 分钟/月
	文件存储	单个实例 $\geq 99.95\%$ ，不可用时间须 ≤ 21.9 分钟/月
	表格存储	单个实例 $\geq 99.95\%$ ，不可用时间须 ≤ 21.9 分钟/月
	日志存储	单个实例 $\geq 99.95\%$ ，不可用时间须 ≤ 21.9 分钟/月
网络服务	弹性公网 IP	单个实例 $\geq 99.95\%$ ，不可用时间须 ≤ 21.9 分钟/月
	NAT 网关	单个实例 $\geq 99.95\%$ ，不可用时间须 ≤ 21.9 分钟/月
	负载均衡	单个实例 $\geq 99.95\%$ ，不可用时间须 ≤ 21.9 分钟/月
	DNS	单个实例 $\geq 99.95\%$ ，不可用时间须 ≤ 21.9 分钟/月
	互联网出口带宽	单个实例 $\geq 99.95\%$ ，不可用时间须 ≤ 21.9 分钟/月
数据库服务	MySQL 数据库	单个实例 $\geq 99.95\%$ ，不可用时间须 ≤ 21.9 分钟/月
	MS SQL 数据库	单个实例 $\geq 99.95\%$ ，不可用时间须 ≤ 21.9 分钟/月
	MongoDB 数据库	单个实例 $\geq 99.95\%$ ，不可用时间须 ≤ 21.9 分钟/月
	云数据库-类型 I（兼容 MySQL、Oracle）	单个实例 $\geq 99.95\%$ ，不可用时间须 ≤ 21.9 分钟/月
	云数据库-类型 II（兼容 MySQL）	单个实例 $\geq 99.95\%$ ，不可用时间须 ≤ 21.9 分钟/月
	云数据库-类型 III（兼容标准 SQL）	单个实例 $\geq 99.95\%$ ，不可用时间须 ≤ 21.9 分钟/月
	NoSQL 数据库服务	单个实例 $\geq 99.95\%$ ，不可用时间须 ≤ 21.9 分钟/月
	分布式关系型数据库	单个实例 $\geq 99.95\%$ ，不可用时间须 ≤ 21.9 分钟/月
	数据库管理服务	单个实例 $\geq 99.95\%$ ，不可用时间须 ≤ 21.9 分钟/月
	云分析型数据库	单个实例 $\geq 99.95\%$ ，不可用时间须 ≤ 21.9 分钟/月
大数据服务	大数据计算服务	单个实例 $\geq 99.95\%$ ，不可用时间须 ≤ 21.9 分钟/月
	实时计算服务	单个实例 $\geq 99.95\%$ ，不可用时间须 ≤ 21.9 分钟/月
	搜索服务	单个实例 $\geq 99.95\%$ ，不可用时间须 ≤ 21.9 分钟/月
	大数据开发治理平台	单个实例 $\geq 99.95\%$ ，不可用时间须 ≤ 21.9 分钟/月
	实时数据分发	单个实例 $\geq 99.95\%$ ，不可用时间须 ≤ 21.9 分钟/月
	大屏开发工具	单个实例 $\geq 99.95\%$ ，不可用时间须 ≤ 21.9 分钟/月
	标准版	单个实例 $\geq 99.95\%$ ，不可用时间须 ≤ 21.9 分钟/月

中间件服务	企业级分布式应用服务	单个实例 $\geq 99.95\%$ ，不可用时间须 ≤ 21.9 分钟/月
	应用实时监控服务	单个实例 $\geq 99.95\%$ ，不可用时间须 ≤ 21.9 分钟/月
	云服务总线	单个实例 $\geq 99.95\%$ ，不可用时间须 ≤ 21.9 分钟/月
	流量防护	单个实例 $\geq 99.95\%$ ，不可用时间须 ≤ 21.9 分钟/月
	消息队列	单个实例 $\geq 99.95\%$ ，不可用时间须 ≤ 21.9 分钟/月
	容器服务	单个实例 $\geq 99.95\%$ ，不可用时间须 ≤ 21.9 分钟/月
	API 网关	单个实例 $\geq 99.95\%$ ，不可用时间须 ≤ 21.9 分钟/月

(三) 服务能力

1. 技术路线和分区要求

建成支持 X86 或 ARM 技术路线的三种不同网络环境的业务区，即：政务外网区、互联网区、行业专网业务区。

2. 自主可控关键核心技术建设要求

- 1) 政务云区物理服务器扩容和替换须采用通过相关机构的安全可靠测评的产品。
- 2) 云服务器须提供通过相关机构的安全可靠测评的操作系统。

3. 非自主可控关键核心技术建设要求

采用业内领先的软硬件技术，提供包括弹性计算服务、开放存储服务、关系型数据库服务、开放结构化数据服务等在内的一系列云服务。

4. 网络要求

每个云区保证提供政务外网至政务服务区互联服务 2 条（2*10G 专线），技术要求如下：

- 1) 互联专线服务：提供专线 2 条，每条速率 10G、接口为万兆光口。
- 2) 误码率 $\leq 1e-9$ ；
- 3) 链路延时 $\leq 30ms$ ；
- 4) 封包成功率 $\geq 99.99\%$ ；
- 5) 每条电路具备双路由环保护。

5. 重大应用容灾能力要求（按需）

- 1) 支持应用双活部署，支持统一云资源管理和全业务容灾能力；
- 2) 支持全量和增量数据同步能力；
- 3) 主备之间通过 2 根及以上的传输专线互联，光缆全程分离路由；
- 4) 提供统一容灾管理中心，提供租户化的容灾计划、容灾监控和故障恢复能力。

5) 满足具备异地备份能力，包括支持周期性备份、备份多版本保存、数据恢复、支持对云主机快照全量或增量备份和恢复，支持云数据库物理备份和恢复、支持物理备份，支持全量备份和增量备份等能力。

6. 满足云平台（云区）安全要求

1) 云平台（云区）安全防护系统应支持软件化部署，具有高可用设计和弹性扩展能力；

2) 云平台（云区）安全防护系统应能够实现与云平台（云区）联动，用户业务上线后即自动提供安全保障服务；

3) 云平台（云区）应提供基础的安全审计功能，支持的审计内容包括但不限于网络设备日志审计、用户行为审计、数据库审计、运维审计等，日志保存时间不低于 6 个月。

7. 云平台上线验收要求

服务能力验证包括以下方面：

1) 机房基础环境。需满足招标文件中 IDC 机房的要求。

2) 运营运维能力。投标人需具备政务云服务的运营运维能力，包括但不限于配套的管理体系、人员队伍、技术力量、设备工具等。

3) 基本服务覆盖。云平台应至少能提供包括云主机、云存储、云数据库或国产化数据库、云负载均衡和国产化中间件等基础服务

4) 网络安全技术防护能力。云平台应符合国家安全政策法规，须通过三级等级保护测评（测评得分不低于 90 分）并提供佐证材料。

5) 统一纳管并接入 IRS。云平台配合通过衢州市统一运营管理平台纳管并接入 IRS，具备云平台的统一纳管、资源申请、自动开通、账单分析、运营分析、资源效能分析等功能。

8. 云平台后续服务要求

1) 相应云区在服务能力验收后 9 个月内通过国家密码应用安全性测评，并提供佐证材料。

2) 服务期内，各云区须每年开展并通过国家网络安全等级保护三级测评（测评得分不低于 90 分）和密码应用安全性评估（测评得分不低于 60 分）。网络安全需动态满足国家、省最新文件要求，增添必要网络安全设备，及时更新策略规则库。

9. 云平台迭代优化要求

相同品牌的云平台各节点应保持版本同步，并在服务期内免费迭代升级。不同品牌的云平台应按采购人要求做好相互配合。

（四）付款周期、计费方式

1. 支付周期

服务费用按年支付，上年度最终支付费用确定后一个月内完成支付最迟不晚于当年的12月31日。

2. 上年度最终支付费用确定方式

按上年度资源、服务实际使用情况计算，最终支付费用由采购人组织第三方审计和服务考核（详见考核管理办法）后确定。

3. 计费方式

具体结算金额按服务期内资源实际使用量结算，最终结算金额不得超过合同金额，若最终结算金额超过合同金额，则超过部分不予支付。具体按以下规则计费：

1) 政务云服务（含采购人审批的渗透测试、代码审计、攻防演练等服务）的费用由采购方统一付费。

2) 云租户（指使用云资源的市本级单位，不含采购人）所选的渗透测试、代码审计、攻防演练等安全服务由云租户自行支付（可参考本次成交的服务单价）。

3) 政务云服务的开通、变更、结束，均从采购人业务审批完成的次日开始（结束）计费。

4) 渗透测试、代码审计、漏洞扫描、攻防演练等服务，在提供相关佐证材料后按以下方式计费：实际服务次数×服务结算单价。

5) 投标人的投标价为服务结算单价。若浙江省（含各地市）政务云服务平均资费发生持续变动，双方可协商调整服务结算单价。

（五）考核管理办法

考核满分100分，包含六方面内容：运维考核、平台可用性考核、利用率与业务迁移考核、使用单位满意度调查、采购人满意度评价、安全保障条款（扣分项）。采购人每年邀请专家对投标人本年度服务质量进行评分，根据专家评分、使用单位满意度调查及采购人满意度评价结果，计算总得分，并以此作为服务费给付额度定档的重要标准。

总得分 (X)	服务费支付额度 (Y)
$X \geq 90$ 分	Y=当年审计后的服务费
75 分 $< X < 90$ 分	Y=当年审计后的服务费*[1-(100-X)*1‰]
60 分 $\leq X \leq 75$ 分	Y=当年审计后的服务费*[1-(100-X)*2‰]
$X < 60$ 分	Y=当年审计后的服务费*[1-(100-X)*10‰]

本办法中扣除比例的基数，以当年审计后的服务费为准，且 3 年结算费用不超过 1.91 亿元。

一、运维考核（25 分）

运维考核包含三方面内容：驻场服务考核、月度考核、工单考核。

1. 驻场服务考核

驻场服务地点为采购人指定地点，投标人应做好驻场人员的日常考勤管理。投标人应提供内容真实的《衢州政务云平台驻场人员运维周报》和考勤记录。根据驻场人员日常考勤情况，视情评分 0-5 分。

2. 月度考核

（1）每月巡检报告

投标人每月对云计算平台进行现场巡检，填写《衢州政务云平台现场巡检记录表》，每月定期送采购人备案。根据现场巡检和记录表提交情况，视情评分 0-5 分。

（2）每月运维报告

投标人须在每月开始 5 个工作日内，向采购人提交上一个月的《市级单位云资源使用情况》，包括本月整体上云情况，本月新开通、变更、撤销云资源清单、CPU、内存和存储资源利用率、监控插件离线的云服务器清单、数据安全产品使用情况等内容。根据云资源使用报告提交情况，视情评分 0-5 分。

3. 工单考核

投标人须在 3 个工作日内，按照要求完成经采购人审批同意的云资源新增、撤销、变更工单。投标人须在 1 日内响应上云单位提出的咨询、故障、维护等服务工单。根据投标人响应情况，视情评分 0-10 分。

二、平台可用性考核（30 分）

平台可用性考核包含三方面：平台维护、重大事项保障、应急管理。

1. 平台维护

投标人要提供 7*24 小时的平台维护服务。发生故障的，投标人须如实填写《衢州政务云平台故障备案表》，交至采购人备案。根据备案表提交情况、平台维护情况，视情评分 0-9 分。

2. 重大事项保障

重大事项保障时间段内，投标人应提供重大事项保障方案、值班表、每日事项记录等相关材料。根据材料提供情况，视情评分 0-6 分。

3. 应急管理

(1) 应急演练

投标人须制定严谨规范的应急预案，并根据实际工作情况不断完善。投标人根据应急预案，每年至少开展 2 次应急演练，根据应急预案、演练情况，视情评分 0-5 分。

(2) 应急事件处理与报告

当云平台（云区）受到攻击或发生其它突发性事故时，投标人须在 1 小时内向采购人备案，且在 24 小时内恢复正常业务，根据备案及业务恢复情况，视情评分 0-5 分。

(3) 投标人应在应急事件发生后 2 个工作日内，向采购人提交书面报告，根据书面报告提交情况，视情评分 0-5 分。

三、利用率与业务迁移考核（25 分）

利用率与业务迁移考核包含三方面：云资源插件管理要求、云资源利用率和数据安全产品使用率要求、业务迁移要求。

1. 云资源插件管理要求

投标人应协助采购人做好云服务器监控插件在线率管理工作，及时将插件离线的实例情况向采购人报告并协助采购人持续跟踪修复。根据投标人报告的及时程度、配合程度，视情评分 0-8 分。

2. 云资源利用率和数据安全产品使用率要求

投标人应协助采购人做好政务云平台资源和数据安全产品使用日常监管工作，对于资源利用率不满足省级相关考核标准或数据安全产品申请后使用不到位的部门，应及时向采购人报告并协助采购人持续跟踪整改。根据投标人报告的及时程度、配合程度，视情评

分 0-8 分。

3. 业务迁移要求

租户更换云平台，需向采购人提交迁移申请单。为保证租户业务与服务连续性，在迁移申请单审批通过后，投标人应配合租户进行业务迁移与服务上线工作，根据投标人配合程度，视情评分 0-9 分。

具体时限要求为：30 个资源实例以内的应用，迁移时间不超 30 个工作日，超过 30 个资源实例的应用，迁移时间不超过实例数量*1.1（四舍五入）个工作日。如因投标人原因导致迁移超期，每超过 1 个工作日，扣 0.1 分，9 分扣完为止。

四、使用单位满意度调查（10 分）

采购人每年向市级政务云资源使用单位开展满意度调查，根据调查结果进行评级打分 0-10 分。

五、采购人满意度评价（10 分）

采购人对投标人项目负责人、驻场人员等项目人员的服务态度、服务质量、响应速度、沟通协作等方面进行综合评价，根据评价结果进行评级打分 0-10 分。

六、安全保障条款（扣分项）

1. 发生一起因投标人原因造成的《浙江省信息系统网络安全事件隐患分级分类指南（试行）》中所指的 III 级（较大）及以上安全事件并被省级主管部门通报扣除相应云区当年服务款的 3%，IV 级（一般）安全事件并被省级主管部门通报扣除相应云区当年服务款的 1%。以上扣除总金额不超过相应云区当年服务款的 20%。考核期内累计因投标人造成 3 次及以上安全事件，采购人有权解除服务合同，并由投标人承担相应损失。

2. 投标人应做好政务云平台安全保障工作，对于省级及以上单位组织的网络安全攻防演练中出现的安全隐患（以省级及以上单位的通报文件为准），按照以下条例处理：

（1）政务云平台被获取云管理平台控制权、获取骨干网络设备控制权限、被突破网络边界，进入逻辑隔离业务内网或强隔离业务内网，且未发现或防守无效的视为特别重大安全事件，每发现 1 次扣除 20 万元，当年考核总分扣 2 分；

（2）被获取网络安全设备（包括但不限于防火墙、堡垒机、IDS、审计设备、WAF 等）和运维机服务器权限、以云侧资产漏洞作为入口或跳板导致核心生产网（市公共数据平台、区县公共数据平台、资源平台等核心业务系统网络）失陷的，且未发现或防守无效的视为

重大安全事件，每发现 1 次扣除 10 万元，当年考核总分扣 1 分；

(3) 被获取堡垒机、运维机服务器权限或其它安全产品权限但未造成严重影响的，视为一般安全事件，每发现 1 次扣除 5 万元，当年考核总分扣 0.5 分。

(六) 项目培训要求

1. 为确保本项目得以顺利实施、正常运行和使用，投标人必须为招标人提供平台管理系统使用、系统操作和管理维护培训，培训规模按用户实际需求为准，培训形式包括客户现场培训、课堂培训，投标人必须列明相应的培训课程。

2. 投标人应在投标文件中提供详细的培训计划，包括培训项目、人数、地点、日程、资料、其它等详细内容，为所有被培训人员提供培训用文字资料和讲义等相关用品。

3. 所有培训费用（含培训教材费），已包括在投标总价中。

4. 实际培训时间、人数和地点按投标人与项目招标人商定的为准。

(七) 售后服务要求（驻场人员，服务团队）

▲总体服务要求：提供不少于 10 人的专职服务团队（包括运营、技术、安全等服务人员），其中 3 人常驻采购人指定地点开展服务。驻场服务地点为采购人指定地点，投标人应做好驻场人员的日常考勤管理。

1. 平台运维服务

云服务商应成立云平台专业运维服务团队，包含云服务商自有团队、原厂（授权）技术服务团队、安全厂商团队，负责云平台的整体运维。云平台专业运维服务团队至少由云服务商、原厂（授权）技术服务商、安全厂商组成。

运维服务内容包括资源管理、日常监控、故障处理、安全管理、运行分析。根据服务对象不同，可分为平台侧运维服务要求和租户侧运维服务要求。

(1) 平台侧运维服务

平台侧运维服务包含平台日常运维、容灾和管理等服务。

平台侧容灾演练服务：每年至少提供一次平台侧容灾演练服务，每次不少于 2 个应用系统，应用系统由招标人按实际情况指定。

(2) 租户侧运维服务

租户侧运维服务包含租户日常运维服务和容灾运维服务。租户日常运维服务包含云资源服务开通、业务系统安全检测、安全配置审核、域名备案指导、日常监控运维、安全运

维；租户容灾运维服务包含对容灾业务应用云资源巡检、容灾保护组配置等。

2. 日常运行监控

云服务商应提供 7*24 小时的监控、值班值守和服务台热线。服务台作为事件管理平台的入口，及时响应云平台用户的各类请求，根据事件的具体情况负责事件的登记、升级、跟踪直至关闭。

按照监控要求和规范，负责执行 7*24 小时监控服务，包括邮件、电话等告警服务。

7*24 小时监控内容包括服务器、存储、网络、云平台、虚拟机，虚拟机的监控服务基于用户自愿的原则。

7*24 小时值班值守服务，加强巡查监测，遇到故障等突发事件，必须立即启动应急响应。

3. 技术支持服务

当云平台系统发生问题时，远程技术支持应立即响应并在半小时内准备好相应的测试工具和环境，通过检查和了解用户系统问题判断问题原因，提出解决方案并及时向用户反馈，并完整记录远程登录和支持过程。

对于通过远程操作不能解决的问题，相关系统工程师 1 小时内到现场进行处理。正常处理完故障后，对于简单性和常见故障在解决故障后 24 小时内提供故障分析报告，对于特殊性故障在一周内提供故障报告。

4. 平台故障处置

根据故障的严重程度和影响业务程度的不同，故障级别由高到低分为一级故障、二级故障和三级故障。

一级故障：主要指设备在切换中出现系统瘫痪或业务服务中断，导致设备的基本功能不能实现或全面退化的故障；或在运行中出现的故障具有潜在的系统瘫痪或服务中断的危险，并可能导致设备的基本功能不能实现或全面退化；业务不能提供正常服务并有大量用户报障。

二级故障：主要指设备在切换中出现的严重影响服务的情况，导致系统性能或服务部分退化的故障；断续或间接地影响系统功能，业务部分功能失效，少量用户报障。

三级故障：设备故障或隐患，暂不影响业务的正常提供。

故障处理过程中做好故障现象和故障处理情况的记录，故障恢复后根据故障的级别和

复杂程度在规定时间内提交故障分析专题报告（一级故障在故障发生的 24 小时内提交，二、三级故障在 48 小时内提交），分析内容包括故障现象、故障类型、故障起始时间、响应时间、修复时间、故障原因、故障处理情况及结果、故障处理人及今后的预防措施等。

5. 用户系统故障处置

当使用单位系统出现故障，需要云服务商提供运行维护与支持服务时，应立即作出实质性响应，核实故障情况、收集故障信息，并且立即派出专业经验丰富的技术人员赶到故障现场，分析故障原因，确定故障点，根据故障类型和使用单位的需求，进行故障排除。

6. 维护日志服务

云服务商每周对设备故障情况、厂商维护日志以及现场人员的维护日志进行分析；采购人可通过定期检查、随机抽查等方式检查维护记录。

7. 系统巡检服务

云服务商应提供日常巡检，云平台原厂商每季度开展一次深度巡检服务，现场听取采购人意见，及时发现设备运行中出现的隐患，提供巡检服务报告，并进行整改，通过系统调整等手段，减少设备发生故障的概率，保证云平台设备稳定、高效运行。

8. 平台升级服务

当云平台以及容灾管理平台发布重要版本，应及时与采购人沟通，为采购人进行免费升级。升级过程中要评估好更新风险，在进行云平台及容灾管理平台版本升级时，要确保升级过程各项业务正常运行。

9. 原厂技术支持

云平台原厂应针对业务平台的特性，组织专家组成虚拟团队提供服务，对于云平台在维护工作中碰到的有关设备技术、业务的故障、非故障类问题，提供技术支持，保证云平台关于设备的技术性问题得到及时、有效的解决。

第四章 合同主要条款

项目名称:

项目编号:

甲方:

乙方:

甲、乙双方根据项目名称公开招标的结果，签署本合同。

一、服务内容

1. 衢州市政务云服务（XC 部分）

1) 基础云资源服务

基于“两地三中心”架构体系，建设基于自主可控关键核心技术的云平台，提供计算、存储、网络、国产数据库、国产中间件、国产操作系统、云原生数据库等服务。

2) 应用服务

提供企业级分布式应用、应用实时监控、云服务总线、流量防护、性能测试、消息队列、容器服务、API 网关等服务。

3) 大数据服务

提供大数据计算、实时计算、搜索服务、智能报表、实时数仓、数据分析等大数据相关服务。

4) 容灾备份服务

提供异地备份服务。

5) 安全服务

提供网络安全（漏洞扫描、主机安全防护、WEB 应用防火墙等）、应用安全（代码审计、高危隐患和安全事件预警等）、数据安全（数据库权限管控系统、数据库审计等）、攻防演练（攻防演练服务、重要活动时期安全保障等）、渗透服务等安全服务。

6) 机柜托管服务

提供机柜托管服务。

2. 衢州市政务云服务（非 XC 部分）

1) 基础云资源服务

提供云主机计算、块存储、对象存储、云数据库等基础云资源服务。

2) 大数据服务

提供大数据服务、大数据开发治理等服务。

3) 其他服务

提供云产品备份、分布式应用、主机托管等服务。

4) 安全服务

提供网络安全（漏洞扫描、云堡垒机、日志审计、WEB 防火墙等）、渗透服务、应用安全（代码审计、主机安全防护等）、数据安全等服务（数据库权限管控、数据库审计、静态脱敏等）。

二、合同金额及计费规则

本合同金额为（大写）：_____万元（¥_____元）人民币。具体结算金额按服务期内资源实际使用量结算，最终结算金额不得超过合同金额，若最终结算金额超过合同金额，则超过部分不予支付。具体按以下规则计费：

1. 政务云服务（含甲方审批的渗透测试、代码审计、攻防演练等服务）的费用由采购方统一付费。

2. 云租户（指使用云资源的市本级单位，不含甲方）所选的渗透测试、代码审计、攻防演练等安全服务由云租户自行支付（可参考本次成交的服务单价）。

3. 政务云服务的开通、变更、结束，均从甲方业务审批完成的次日开始（结束）计费。

4. 渗透测试、代码审计、漏洞扫描、攻防演练等服务，在提供相关佐证材料后按以下方式计费：实际服务次数×服务结算单价。

5. 各项服务结算单价见附件一。若浙江省（含各地市）政务云服务平均资费发生持续变动，甲乙双方可协商调整服务结算单价。

三、技术资料

1. 乙方应按招标文件规定的时间向甲方提供有关技术资料。

2. 没有甲方事先书面同意，乙方不得将由甲方提供的有关合同或任何合同条文、规格、计划、图纸、样品或资料提供给予履行本合同无关的任何其他人。即使向履行本合同有关

的人员提供，也应注意保密并限于履行合同的必需范围。

四、知识产权

乙方应保证所提供的服务或其任何一部分均不会侵犯任何第三方的知识产权。

五、履约保证金

合同签订前，乙方向甲方交纳中标价 1%的履约保证金_____元，大写：_____（以现金、电汇或保函的形式）。电汇形式的服务期满后，乙方无任何违约、赔偿等情况的，甲方在 30 日内将履约保证金原额无息退还给乙方。以保函形式提供的，保函有效期应在合同期限上不少于 6 个月且保函到期时合同未履行完毕的，乙方应在保函到期前完成续保。

六、转包或分包

本项目不得以任何形式转包或分包。

七、网络和数据安全

1. 总体要求。乙方要严格按照《中华人民共和国网络安全法》《中华人民共和国个人信息保护法》《中华人民共和国数据安全法》《关键信息基础设施安全保护条例》《浙江省信息技术外包网络安全管理办法》《浙江省公共数据条例》《网络数据安全风险评估实施指引》相关要求，对云平台及数据进行安全保护和管理。

2. 网络安全要求。乙方需按照甲方的网络安全管理制度，严格落实网络安全责任，执行日常安全运维、检查制度，确保不发生信息泄密、重大安全漏洞等安全事故，需要开展现场长期服务的乙方，需派驻现场专职人员，其主要职责包括：负责按照国家及甲方的网络安全管理要求，配合甲方开展派驻现场的安全管理，确保不发生违规行为，接受甲方的监督。乙方网络安全管理人员发生变更时，应在变更前一周将有关变更信息报送甲方。甲方有权督促指导乙方及人员遵循甲方的安全管理制度和规范，将安全要求合同内容，纳入双方合作协议，定期组织对乙方进行网络安全监督。

3. 数据安全要求。在合作过程中，如有不可避免地接触到甲方的数据资料、经营信息等各类敏感信息及秘密（下面简称敏感信息），需要甲方进行全程评估及监督，保证不损害敏感信息的保密性、完整性、可用性、真实性、可核查性、可靠性、防抵赖性。在合作过程中，乙方需按照不同权限查看相应的数据，原则上无权修改数据。如工作需要，需甲方指派人员对乙方修改数据行为进行监督评估。乙方对于数据内容和数据结构进行变更前，应提前向甲方提出变更申请，以避免发生数据混乱。乙方有责任配合甲方开展数据备份，

数据备份采取定期备份与动态备份相结合的原则。要确保备份数据的完整性和正确性，若数据备份存在问题，应及时把问题反馈至甲方。乙方在工作中产生的敏感数据，在需要销毁时由甲方负责执行，销毁时须有数据生产部门和数据使用部门相关人员监督销毁。

八、服务期限

服务期 36 个月（自甲方组织服务能力验证通过后起计，最迟不晚于 2024 年 12 月 31 日）。

服务能力验证包括以下方面：

1. 机房基础环境。需满足招标文件中 IDC 机房的要求。
2. 运营运维能力。乙方需具备政务云服务的运营运维能力，包括但不限于配套的管理体系、人员队伍、技术力量、设备工具等。
3. 基本服务覆盖。云平台应至少能提供包括云主机、云存储、云数据库或国产化数据库、云负载均衡和国产化中间件等基础服务
4. 网络安全技术防护能力。云平台应符合国家安全政策法规，须通过三级等级保护测评（测评得分不低于 90 分）并提供佐证材料。
5. 统一纳管并接入 IRS。云平台配合通过衢州市统一运营管理平台纳管并接入 IRS，具备云平台的统一纳管、资源申请、自动开通、账单分析、运营分析、资源效能分析等功能。

九、合同履行地点

1. 履行地点：浙江省衢州市

十、款项支付

1. 支付周期

服务费用按年支付，上年度最终支付费用确定后一个月内完成支付最迟不晚于当年的 12 月 31 日。

2. 上年度最终支付费用确定方式

按上年度资源、服务实际使用情况计算，最终支付费用由甲方组织第三方审计和服务考核（考核管理办法见附件二）后确定。

3. 甲方应将合同款支付至乙方指定的如下银行账户：

开户名称：_____

开户银行：_____

账 号：_____

十一、税费

本合同执行中相关的一切税费均由乙方负担。

十二、质量保证及后续服务

1. 乙方应按招标文件规定向甲方提供服务。

2. 乙方提供的服务成果在服务期内发生故障，乙方应负责及时排除故障。对达不到要求者，根据实际情况，甲方有权按以下方式处理：

(1) 贬值处理：按考核管理办法执行；

(2) 解除合同。

3. 在服务期内，乙方应对出现的质量及安全问题负责处理解决并承担一切费用。

4. 运维团队要求。乙方提供不少于 10 人的专职服务团队（包括运营、技术、安全等服务人员），其中 3 人常驻甲方指定地点开展服务。如在使用过程中发生问题，乙方团队在接到甲方通知后在 30 分钟内到达故障现场。

5. 相应云区在服务能力验收后 9 个月内通过国家密码应用安全性测评，并提供佐证材料。

6. 服务期内，各云区须每年开展并通过国家网络安全等级保护三级测评（测评得分不低于 90 分）和密码应用安全性评估（测评得分不低于 60 分）。网络安全需动态满足国家、省最新文件要求，增添必要网络安全设备，及时更新策略规则库。

7. 政务云服务等级协议（SLA）指标应满足附件三要求。

(1) 服务周期内，各产品实例如发生故障，故障不可用时间超过 21.9 分钟，每发生一次，甲方有权扣除该实例当月费用等额的金额，直到服务周期内该实例费用扣完为止。

(2) 服务周期内，各产品实例如发生故障，故障不可用时间尚未超过 21.9 分钟，但同一实例每累计两次故障，甲方有权扣除该实例第 2 次故障当月费用等额的金额，直到服务周期内该实例费用扣完为止。

(3) 故障次数超出扣款：服务周期内，每月各产品实例发生故障（含激活 SLA 的故障和未激活 SLA 的故障）的次数应不超出当月云实例总数的万分之一，如超出，每超出万分之一，甲方有权扣除本项目当月结算费用的 1%；全年累计故障总次数（含激活 SLA 的

故障和未激活 SLA 的故障) 应不超出项目验收时云上总实例数量的千分之一, 如超出, 每超出千分之一, 甲方有权扣除本项目结算费用的 1%。

(4) 云平台可靠性未达标扣款: 服务周期内, 验收时云平台可靠性应达到 99.95%, 如未达到, 指标每下降 0.01%, 甲方有权扣除本项目结算费用的 0.2%。

十三、违约责任

1. 甲方无正当理由拒绝接受服务的, 甲方向乙方偿付合同款项百分之五作为违约金。

2. 甲方无故逾期验收和办理款项支付手续的, 甲方需向乙方按天支付违约金(以逾期金额为基数按照违约发生时同期贷款市场报价利率<LPR>向乙方支付违约金)。

3. 乙方未能如期提供服务的, 每日向甲方支付合同款项的万分之一作为违约金。乙方超过约定日期 10 个工作日仍不能提供服务的, 甲方可解除本合同。乙方因未能如期提供服务或因其他违约行为导致甲方解除合同的, 乙方应向甲方支付合同总值 5%的违约金, 如造成甲方损失超过违约金的, 超出部分由乙方继续承担赔偿责任。

十四、不可抗力事件处理

1. 在合同有效期内, 任何一方因不可抗力事件导致不能履行合同, 则合同履行期可延长, 其延长期与不可抗力影响期相同。

2. 不可抗力事件发生后, 应立即通知对方, 并寄送有关权威机构出具的证明。

3. 不可抗力事件延续 120 天以上, 双方应通过友好协商, 确定是否继续履行合同。

十五、诉讼

双方在执行合同中所发生的一切争议, 应通过协商解决。如协商不成, 可向甲方所在地法院起诉。

十六、合同生效及其它

1. 合同经双方法定代表人或授权代表签字并加盖单位公章后生效。

2. 合同执行中涉及采购资金和采购内容修改或补充的, 须签订书面补充协议报部门纪委备案, 方可作为主合同不可分割的一部分。

3. 本合同未尽事宜, 遵照《民法典》有关条文执行。

4. 本合同一式陆份, 具有同等法律效力, 甲乙双方各执叁份。

甲方（公章）：

乙方（公章）：

法定（授权）代表人（签字）：

法定（授权）代表人（签字）：

地址：

地址：

电话：

电话：

开户银行：

开户银行：

账号：

账号：

签订日期： 年 月 日

附件一：各项政务云服务单价（根据中标单位所报折扣率及折后单价填写）

附件二：考核管理办法（详见第三部分采购需求服务质量考核办法）

附件三：政务云平台服务等级协议（SLA）指标（详见第三部分采购需求）

第五章 评标办法

一、评审小组的组成

1. 评审小组由 7 人及以上单数组成，由采购人代表（2 人）和评审专家（5 人）组成，评审专家从专家库里随机抽取，评审小组对投标文件进行评审。采购人代表负责对本项目评审质量和结果的审查，但不得担任评审小组负责人。

2. 询标期间，投标人法定代表人（负责人）或法定代表人（负责人）委托人必须全程在线，负责解答有关事宜，确保评标顺利进行。

二、评标原则

1. 投标人得分由技术商务分和报价分合计组成，满分为 100 分。

2. 技术商务分与报价分合计得分最高者前三名为中标候选人，总分相同时，价格低者优先。报价得分、技术商务得分均相同的，则现场抽签确定。

3. 评审小组根据采购文件和投标文件，结合技术商务评分细则对各投标人的技术商务部分进行评审。评审小组各成员所评分值的算术平均值即为各投标人的技术商务分值（计算时四舍五入保留两位小数）。

4. 评定结果经采购人确定后，采购代理机构在中标人确定之日起 2 个工作日内在指定的媒体上公告中标结果同时将以书面形式发出中标通知书。

三、注意事项

评审时评审小组认为投标人的报价明显低于其他通过符合性审查投标人的报价，有可能影响产品质量或者不能诚信履约的，应当要求其在评标现场合理的时间内提供书面说明，必要时提交相关证明材料；投标人不能证明其报价合理性的，评审小组应当将其作为无效投标处理。

四、评分标准

（1）报价评分（20 分）

本项目投标报价以折扣率的形式进行报价（按第三章采购内容及要求“二、服务清单及限价”中每项服务的最高限价的综合折扣比例，用百分比表述，保留小数点后前两位的数字），满足评标要求且折扣率最低的为基准价，投标报价得分=(基准价 / 投标报价) × 20，四舍五入，保留两位小数。

（2）技术商务分（80 分）

序号	评审因素	评审标准	分值
1	项目业绩	2021年1月1日（以合同签订时间为准）以来，投标人（含牵头人单位和联合体成员单位）实施的类似项目的成功案例提供一个得1分。须提供项目合同扫描件。	0-1分
2	公司资质	投标人（含牵头人单位和联合体成员单位）具有有效的信息技术服务管理体系认证（ISO/IEC20000）、信息安全管理体认证（ISO/IEC27001）、云服务信息安全管理体认证（ISO/IEC27017）、信息系统安全集成二级及以上服务资质证书。每提供一个得1分，最高得4分。须提供证书扫描件，未提供不得分。	0-4分
3	拟派项目组成员	1. 拟派运维服务团队的项目经理同时具备全国计算机软考类信息系统项目管理师（高级）证书、人社部门颁发的通信工程师证书、注册信息安全专业人员（CISP）的得3分，同时具备其中两本证书的得1分，其余不得分。 2. 拟派运维服务团队的技术负责人同时具备全国计算机软考类系统集成项目管理师证书、ITIL证书的，得1分，其余不得分。 3. 项目团队人员具有人社部门颁发的通信中级及以上证书，每提供一本得0.5分，本项最多得4分。 【以上人员须提供有效的相关证书复印件（或扫描件）和近6个月内缴纳的社保证明复印件（或扫描件），并加盖投标人电子公章，否则不得分。】	0-8分
4	总体设计方案	根据投标人对本项目需求设计的总体方案进行综合打分。 投标人提供的总体设计方案合理、总体技术架构和关键技术设计合理、功能后期延展性强、与项目实际需求契合度高的得5-7分； 投标人提供的总体设计方案较合理、总体技术架构和关键技术设计较合理、功能后期延展性较强、与项目实际需求契合度较高的得3-5（不含）分； 投标人提供的总体设计方案基本合理、总体技术架构和关键技术设计基本合理、功能后期延展性一般、与项目实际需求契合度较低的得0-3（不含）分； 未提供内容的不得分。	0-7分
5	详细设计方案	根据投标人模块的详细设计方案情况进行综合打分。 设计方案合理、项目需求符合程度高、可实施性强的得6-9分； 设计方案较合理、项目需求符合程度较高、可实施性较强的得3-6（不含）分； 设计方案基本合理、项目需求符合程度一般、可实施性一般的得0-3（不含）分； 未提供内容的不得分。	0-9分
6	云计算平台功能演示	1. 虚拟专有云（VPC）具有IPV6地址的功能，具备ECS可通过IPV6地址访问互联网的IPV6服务，具备ECS作为服务端IPV6地址提供给互联网IPV6客户端访问，同时具备云服务器设置IPV6公网仅主动出规则，即经IPV6地址可主动访问IPV6网络，外部IPV6终端主动发起的访问不通。	0-20分

		<p>根据演示内容进行综合打分： 演示内容详细、步骤清晰且符合招标文件要求的得 4-6 分； 演示内容较符合招标文件要求的得 2-4（不含）分； 演示内容基本符合招标文件要求的得 0-2（不含）分； 不演示不得分。</p> <p>2. 具备离线任务管理、监报告警的功能，任务运维管理支持两种模式可供用户选择，包括列表模式和 DAG 模式。监报告警是调度任务的监控保障系统，具备基线告警和自定义告警两种方式。当任务出现错误或者延迟产出的时候，系统会通过预定义的方式告知用户任务状态。用户可以按照自己定义的规则来配置告警规则。</p> <p>根据演示内容进行综合打分： 演示内容详细、步骤清晰且符合招标文件要求的得 4-6 分； 演示内容较符合招标文件要求的得 2-4（不含）分； 演示内容基本符合招标文件要求的得 0-2（不含）分； 不演示不得分。</p> <p>3. 负载均衡提供监听级别的访问控制，基于监听配置 IP 地址段白名单，只有在白名单中的 IP 地址才允许访问负载均衡。</p> <p>根据演示内容进行综合打分： 演示内容详细、步骤清晰且符合招标文件要求的得 3-4 分； 演示内容较符合招标文件要求的得 1-3（不含）分； 演示内容基本符合招标文件要求的得 0-1（不含）分； 不演示不得分。</p> <p>4. 在高安全场景，具备基于双因子认证，保障云管理安全。具备云主机设备的直通或重定向，用户申请虚拟机时，可以申请将 USB 等设备映射给虚拟机使用。具备为云主机挂载 CD 驱动器（光驱）和 ISO 镜像，用于系统或远程软件安装。</p> <p>根据演示内容进行综合打分： 演示内容详细、步骤清晰且符合招标文件要求的得 3-4 分； 演示内容较符合招标文件要求的得 1-3（不含）分； 演示内容基本符合招标文件要求的得 0-1（不含）分； 不演示不得分。</p> <p>▲1、演示介绍视频存储在 U 盘介质密封在信封内（信封封口处须加盖单位公章）提供给招标代理公司（联系人：吕锋；联系电话 15305707858），要求在 2024 年 8 月 29 日 17：30 分前自行送往衢州市弈谷文体城二期 3-1 二楼，为避免不必要的麻烦，视频 U 盘不接收邮寄形式递交，逾期或以邮寄形式递交或未密封加盖公章的均不予接受，因此造成的后果，由投标人自行承担，不提供不得分。</p> <p>▲2、系统演示介绍视频时长不得超过 15 分钟整，如超过 15 分钟整，本项不得分。</p>	
7	项目理解	根据投标人对衢州原有政务云现状和用户需求的了解情况，包括（机柜系统、空调系统、UPS 系统、网络系统、服务器数量、SLB 数量、存储容量、数据库、上云应用情况、上云企业数量	0-6 分

		等），并提供本次云平台设备选型说明（茁壮性、适用性、稳定性等方面进行比较和选择的理由）进行综合打分。 对原有平台充分了解，选用的云平台技术先进、稳定、安全，对用户需求理解充分、贴合实际的得 4-6 分； 对原有平台有一定了解，选用的云平台较为先进、稳定、安全，对用户需求有理解较为充分、较为贴合实际的得 2-4（不含）分； 对原有平台不了解，选用的云平台性能一般，对用户需求有理解不充分、不贴合实际的得 0-2（不含）分。 未提供内容的不得分。	
8	项目实施进度计划、测试方案	根据投标人提供的项目实施进度计划、测试方案情况进行综合打分。 提供的实施进度计划、测试方案详细完整，贴合项目或优于项目实际需求的得 8-10 分； 提供的实施进度计划、测试方案较详细完整，较贴合项目的得 4-8（不含）分； 提供的实施进度计划、测试方案一般，基本满足实际需求的得 0-4（不含）分； 未提供内容的不得分。	0-10 分
9	售后服务方案	根据投标人提供的售后服务方案（包括维护期、服务方式、质保期内现场响应时效、人员配置、应急响应）情况进行综合评分。 方案描述、响应措施合理，实际可行的得 5-6 分； 方案描述、响应措施较为合理，可行性一般的得 2-5（不含）分； 方案描述、响应措施一般，可行性较弱的得 0-2（不含）分。 未提供内容的不得分。	0-6 分
10	人员培训计划	投标人针对本项目提供的人员培训计划合理规范，培训课程具体丰富，师资配备，培训方案与项目对应需求的满足程度等。 培训计划合理规范、培训方案与项目对应需求的满足度高的得 3-4 分； 培训计划较合理规范、培训方案与项目对应需求的满足度较高的得 2-3（不含）分； 培训计划基本合理规范、培训方案与项目对应需求的满足度一般的得 0-2（不含）分； 未提供内容的不得分。	0-4 分
11	合理化建议	投标人就本项目情况的理解，提出项目存在的问题及合理化建议或措施。 对系统运行、使用有较大提升作用的得 4-5 分； 对系统运行、使用有一定提升作用的得 2-4（不含）分； 对系统运行、使用有较小提升作用的得 0-2（不含）分； 未提供内容的不得分。	0-5 分

第六章 应提交的有关格式范例

一、投标文件封面

资格审查文件

项目名称： _____

项目编号： _____

投标人： _____（盖单位公章）

日期： _____年 _____月 _____日

1. 供应商基本情况表

供应商信息			
企业名称			
性质	单位 <input type="checkbox"/>		个人 <input type="checkbox"/>
统一社会信用代码		注册资金	
法定代表人		身份证号码	
通信地址		邮政编码	
公司电话		传真	
公司网址		电子邮箱	
开户银行及账号			
企业资质			
权威认证			
企业获奖（如有）			
备注			
供应商联系人信息			
姓名		手机	
固定电话		电子邮箱	
企业简介：（可另附页或企业对外宣传手册）			

法定代表人或其授权代表：_____（签字或盖章）

投标人名称：_____（公章）

日期：____年__月__日

2. 法定代表人身份证明

投标人名称： _____

单位性质： _____

地址： _____

成立时间： _____年____月____日

经营期限： _____

姓名： _____ 性别： _____ 年龄： _____ 职务： _____

系 _____（投标人名称）的法定代表人。

特此证明。

投标人名称： _____（公章）

_____年 月 日

附：法定代表人身份证复印件

3. 法定代表人（负责人）授权书

衢州市数字产业发展有限公司：

_____（投标人全称）法定代表人（负责人）____授权_____（全权代表姓名）为全权代表，参加贵方组织的_____项目（项目编号：____），并全权处理采购活动中的一切事宜。

法定代表人（负责人）签字或盖章：

投标人名称（公章）：

日期：____年__月__日

附：

授权代表姓名： 性别：

职务： 职称：

详细通讯地址：

电话： 传真：

移动电话：

邮政编码：

法定代表人身份证复印件：

授权代表身份证复印件：

4. 有效期内的营业执照（或事业法人登记证书或其它工商等登记证明材料）
扫描件

5. 符合参加国企采购活动应当具备的一般条件的承诺函

致：_____（采购人）

我方参加_____项目名称（项目编号：_____）采购活动，郑重承诺：

一、符合《衢州市国有企业采购管理办法（试行）》第十五条规定：

(1)具有独立承担民事责任的能力；

(2)具有良好的商业信誉和健全的财务会计制度；

(3)具有履行合同所必需的设备、技术和售后保障等能力；

(4)有依法缴纳税收和社会保障资金的良好记录；

(5)参加采购、招投标等活动前3年内，在经营活动中没有重大违法记录和行贿犯罪记录；

(6)具有法律法规和规范性文件规定的其他条件。

二、未被“信用中国”(www.creditchina.gov.cn)、中国政府采购网(www.ccgp.gov.cn)列入失信被执行人、重大税收违法案件当事人名单、采购严重违法失信行为记录名单。

三、没有下列情形：

单位负责人为同一人或者存在直接控股、管理关系的不同供应商参加同一合同项下的采购活动。

我方对上述承诺的内容事项真实性负责，如有虚假，由我方承担相关法律责任。

法定代表人或其授权代表：_____（签字或盖章）

投标人名称：_____（公章）

日期：____年__月__日

6、联合体协议书

(主办单位名称)_____ (联合体单位名称)_____ 自愿组成联合体，
参加_____ 项目投标。现就有关事宜订立协议如下：

1. (单位名称)_____ 为联合体主办人，(单位名称)_____ 为
联合体成员。

2. 联合体内部有关事项规定如下：

(1) 联合体共同接受业主的指令、指标和通知；

(2) 项目一切工作由联合体主办人负责组织，由联合体各方按内部划分比例：主办人
(所占百分比)、联合体成员_____ (所占百分比) 具体实施；

(3) 联合体将严格按照招标的各项要求，切实执行一切合同文件，共同承担合同的一
切义务和责任，同时按照内部划分的职责，各自承担自身的责任和风险；

(4) 投标工作和联合体在中标后工程实施过程中的有关费用及项目收益按各自承担的
工作量分摊。

(5) 如中标，联合体内部将遵守以下规定：

a. 联合体主办人和成员共同与业主签订合同书，并就中标项目向业主负责有连带的和
各自的法律责任。

b. 联合体主办人负责_____，联合体成员负责_____。
合同价款收付_____。

3. 本协议书自签署之日起生效，在上述(5)a所述的合同书规定的期限之后自行失效；
如中标后，联合体内部另有协议的，联合体主办人应将该协议书送交业主。

4. 本协议书将随投标文件装订，同时联合体各成员再各自持有一份。

主办单位名称：_____ (全称) (盖章)

法定代表人：_____ (签字盖章)

年 月 日

联合体单位名称：_____ (全称) (盖章)

法定代表人：_____ (签字盖章)

年 月 日

二、投标文件封面

技术商务文件

项目名称： _____

项目编号： _____

投标人： _____（盖单位公章）

日期： ____年 ____月 ____日

2. 投标函

致： _____（采购人名称）：

根据贵方 _____ 项目的招标公告（项目编号： _____），签字代表 _____（全名）经正式授权并代表投标人（投标人名称）提交资格审查文件、技术商务文件、报价文件各一份。

据此函，签字代表宣布同意如下：

1. 我方向贵方提交的所有投标文件、资料都是准确的和真实的。
2. 我方已详细审查全部“采购文件”，包括修改文件（如有）以及全部参考资料和有关附件，已经了解我方对于采购文件、采购过程、采购结果有依法进行询问、质疑、投诉的权利及相关渠道和要求。
3. 我方在投标之前已经与贵方进行了充分的沟通，完全理解并接受采购文件的各项规定和要求，对采购文件的合理性、合法性不再有异议。
4. 本投标有效期自开标日起 _____ 日。
5. 如中标，本投标文件至本项目合同履行完毕止均保持有效，本投标人将按“采购文件”及采购法律法规的规定履行合同责任和义务。
6. 我方同意按照贵方要求提供与投标有关的一切数据或资料。
7. 与本投标有关的一切正式往来信函请寄：

地址： _____ 邮编： _____ 电话： _____

传真： _____ 投标人代表姓名： _____ 职务： _____

投标人名称（公章）： _____

开户银行： _____ 银行账号： _____

被授权代表签字： _____

日期： _____ 年 _____ 月 _____ 日

4. 项目组成员汇总表

项目名称：

项目编号：

序号	姓名	性别	职称（或资质）	拟派岗位	承诺到位时间
1					
2					
3					
4					
5					

8. **备注：**▲乙方提供不少于 10 人的专职服务团队（包括运营、技术、安全等服务人员），其中 3 人常驻甲方指定地点开展服务。如在使用过程中发生问题，乙方团队在接到甲方通知后在 30 分钟内到达故障现场。

投标人（盖章）：

法定代表人或其授权代表人（签字或盖章）：

日 期：

5. 技术偏离表

项目名称：

项目编号：

序号	招标文件技术规范要求	投标人响应详细内容	正/负偏离	偏离说明	投标文件响应页码
1					
2					
3					
...					

注：投标人递交的技术规格书中与招标文件的技术规格书中的要求有不同时，应按要求填写以上表格，否则将认为投标人接受招标文件的全部要求。

投标人（盖章）：

法定代表人或其授权代表人（签字或盖章）：

日期：

三、投标文件封面

报价文件

项目名称：_____

项目编号：_____

投标人：_____（盖单位公章）

日期：____年__月__日

1. 开标一览表

项目名称：_____ 项目编号：_____

序号	内容	单价综合折扣 (%)
1	衢州政务云服务项目	
	我单位承诺最终结算价不超过最高限价，具体结算金额按服务期内资源实际使用量结算。综合折扣率为_____%，大写：_____。	
	<p>特别提醒</p> <p>本项目报价为折扣报价，本项目预算为 19100 万元，具体结算金额按服务期内资源实际使用量结算，结算金额不得超过项目预算。本项目付费范围为衢州市本级党政部门政务云相关业务（不包含县市区业务）。本项目报价计算四舍五入保留小数点后前两位的数字。</p> <p>一、报价方式：响应方参照“第三章第二节服务清单及限价”报出服务折扣。</p> <p>二、折扣定义：即折扣比例（0%<折扣比例<100%，最多保留两位小数），如折扣为 82.56%，则服务结算单价=最高限价×82.56%。各项云服务结算单价=最高限价×对应折扣。各项云服务折扣不同的，可单独列出。</p> <p>三、计费方式</p> <p>具体结算金额按服务期内资源实际使用量结算，最终结算金额不得超过合同金额，若最终结算金额超过合同金额，则超过部分不予支付。具体按以下规则计费：</p> <p>1. 政务云服务（含甲方审批的渗透测试、代码审计、攻防演练等服务）的费用由采购方统一付费。</p> <p>2. 云租户（指使用云资源的市本级单位，不含甲方）所选的渗透测试、代码审计、攻防演练等安全服务由云租户自行支付（可参考本次成交的服务单价）。</p> <p>3. 政务云服务的开通、变更、结束，均从甲方业务审批完成的次日开始（结束）计费。</p> <p>4. 渗透测试、代码审计、漏洞扫描、攻防演练等服务，在提供相关佐证材料后按以下方式计费：实际服务次数×服务结算单价。</p> <p>5. 各项服务结算单价见报价明细表。若浙江省（含各地市）政务云服务平均资</p>	

费发生持续变动，甲乙双方可协商调整服务结算单价。

填写要求：请在本表填写单价综合折扣（单价综合折扣为各项服务单价折扣的平均值），并在表 2 服务折扣明细表填写各项服务单价的具体折扣。

注：1. 报价一经涂改，应在涂改处加盖投标人公章或者由法定代表人或其授权代表签字或盖章，否则其投标作无效标处理。

2. 本项目投标报价包含人工费、交通费、餐费、材料费、税金、政策性风险和提供伴随服务等完成本项目的一切含税费用。如有合同费用漏项，视同已包含在其项目中，合同单价不作调整。

3. 以上数量为暂估数量，最终根据实际数量及成交单价，每年按实结算。

4. 开标一览表中总价须与报价明细表中总价保持一致。

法定代表人或其授权代表：_____（签字或盖章）

投标人名称：_____（公章）

日期：____年__月__日

2. 报价明细表

项目名称：_____ 项目编号：_____

（一）xc 云产品服务

主要内容为衢州市电子政务信息化系统提供所需 xc 计算资源云计算服务。主要内容包含租赁服务主要包括如下基础云服务、中间件服务、安全服务、大数据服务等服务：

产品类别	产品子类	服务名称	计费方式	单位	最高限价 (元/月)	单项折扣 (%)
基础服务	云主机服务	云主机(不含操作系统)	根据核数, 按月计费 (vCPU 主频) =2.2GHz)	core	49.7	
			根据内存, 按月计费	GB	29.85	
	快照	ECS 快照服务	根据存储容量, 按月计费	GB	0.2	
自主可控关键核心技术服务	自主可控关键核心技术软件	国产 WEB 中间件软件	按照配置规格计费 (套), 按月计费	套	830	
		国产操作系统	按照配置规格计费 (套), 按月计费	套	80	
		国产数据库软件	按照配置规格计费 (套), 按月计费	套	2000	
存储服务	块存储服务	高效云盘	根据存储容量, 按月计费	GB	0.63	
		SSD 云盘	根据存储容量, 按月计费	GB	1	
		数据库存储	根据存储容量, 按月计费	GB	1.03	
	对象存储服务	对象存储	根据存储容量, 按月计费	GB	0.2	
	视频云存储	视频云存储	根据存储容量, 按月计费	GB	0.042	
	数据库存储备份服务	数据库备份存储	根据备份存储容量, 按月计费	GB	0.83	
	日志服务	日志服务	根据存储容量, 按月计费	GB	0.33	
网络服务	负载均衡	负载均衡	根据实例个数, 按月计费	1 实例	48	
	VPC	VPC	根据实例个数, 按月计费	1 实例	25.37	
	公网 IP	公网 IP	按 1Mbps/1 个公网 IP 计费	个	37	
	公网带宽	公网带宽	公网带宽每 Mbps 价格 (ipv6), 按月计费。若使用政务外网带宽则不收费。	Mbps	14.17	
				1 实例	29.5	
	云网络服务	NAT 网关	根据实例类型数量+公网 IP 数, 按月计费	性能共享型	13	
		高速通道	根据跨专有网络互通策略数量, 按月计费	每策略	27	
		DNS 服务	根据 Zone 数量+每个 ZONE 的请求次数 (以每万次为 1 个规格递增), 按月计费	计费项 1: Zone 数量	2.07	
	计费项 2: 每个 ZONE 的请求次数			0.8		
	云数据库服务	云数据库-类型 I (兼容 MySQL、Or	云数据库	根据核数, 按月计费	core	210
根据内存, 按月计费				GB	140	

	acle)					
	云数据库-类型 II (兼容 MySQL)	通用型	根据核数, 按月计费	core	45	
			根据内存, 按月计费	GB	35	
		独享型	根据核数, 按月计费	core	59.15	
			根据内存, 按月计费	GB	46.15	
	云数据库-类型 III (兼容标准 SQL)	云数据库	根据核数, 按月计费	core	233	
			根据内存, 按月计费	GB	105	
分布式关系型数据库	分布式关系型数据库	根据核数和内存容量, 按月计费	核数: core 内存容量: GB	101 68		
应用服务	应用实时监控服务	应用实时监控服务	根据应用监控资源包+前端页面监控资源包, 按月计费	应用监控资源包: 1 个 Agent	198	
	消息中间件	消息队列	根据实例 (Topic 数量+消息发送 TPS+消息订阅 TPS) 按月计费	Topic 资源包: 1 个	45	
				消息发送基础包: 1 TPS	2	
				消息发送扩展包: 1 TPS	1.9	
				消息订阅基础包: 1 TPS	1.9	
				消息订阅扩展包: 1 TPS	1.9	
容器服务	容器服务	根据 ECS 节点数量 (不包含资源费用), 按月计费	ECS 节点数量	170		
API 网关服务	API 网关	根据配置规格, 按月计费	每 1RPS	0.9		
大数据服务	大数据服务	大数据计算服务	根据实例开通的 CU 数+存储容量(100G 起步)+增强软件包(非必选), 按月计费	实例开通 CU 数: CU	118	
				存储容量: GB	0.64	
			大数据多维分析服务 (警务节点服务)	实例开通 CU 数: CU	118	
				存储容量: GB, SSD	1	
		大数据消息缓存服务 (警务节点服务)	实例开通 CU 数: CU	118		
			存储容量: GB, SSD	1		
实时计算服务	实时计算服务	根据实例开通的 CU 数, 按月计费	实例 CU 数: CU	129		

	大数据搜索与分析	搜索服务	根据数据节点配置单价及数量+专有主节点配置单价及数量+协调节点配置单价及数量+存储类型及空间及数量，按月计费	数据节点 CPU: 每核	41.16		
				数据节点内存: 每 G	25.4		
				专有主节点 CPU: 每核	90		
				专有主节点内存: 每 G	62		
				协调节点 CPU: 每核	25		
				协调节点内存: 每 G	17		
				存储计费: 高效云盘 (GB)	0.63		
				数据治理与分析	大数据开发治理平台	标准版	根据租户开通的版本按月收费，按套计费
容灾备份服务	异地备份服务	异地备份存储	根据备份存储容量，按月计费	GB	0.15		
		异地备份实例类型	根据备份的实例类型及数量，按月计费	文件备份软件服务 (计算服务)	39		
				应用备份软件服务 (数据库、大数据服务)	153		
传输服务	传输专网	云平台之间容灾用 10G 专线(裸光纤)	根据条数，按年计费	年/条	59200		
安全服务	基础版	网络安全	漏洞扫描	根据云主机数量，按月计费	个	70	
			主机安全防护	根据云主机数量，按月计费	个	64	
			云堡垒机	根据云主机数量，按月计费	个	30	
			日志审计	根据日志源，按月计费	日志源	77.5	
			Web 应用防火墙	根据子域名/IP 数量，按月计费	子域名/IP	200	
			零信任 (VPN 接入)	根据账户数量，按月计费	账户	35	
		应用安全	代码审计	根据系统数量，按次计费	套	6000	
			高危隐患和安全事件预警	根据系统数量，按月计费	套	445.5	
			网络安全流量监测能力服务	根据系统数量，按月计费	套	445.5	
		数据安全	数据库权限管控	根据数据库实例，按月计费	1 实例	1195	

		系统	数据库审计	根据数据库实例，按月计费	1 实例	445	
			动态脱敏	根据数据库实例，按月计费	1 实例	672	
			数据备份	1/GB，按月计费	1/GB	0.42	
			数据库运维及安全评估报告	每月巡检报告，1 次	1 次	600	
			数据库入侵防护（云数据库防火墙）	根据套数，按月计费	1 实例	840	
			攻防演练	攻防演练服务（包含红队（不少于6支红队，每队不少于3人）、紫队、演练方案、平台资源、人员协同、结果报告、演练复盘、加固改进建议报告等）	按次计费	1 次	195000
	选配包	攻防演练	重要活动时期安全保障服务：7*8小时现场值守。（资深专家，具有网络安全保障、攻防演练经验，负责监测预警、研判分析、攻击溯源等）	按每人/天计费	1 人/天	2380	
			渗透服务	渗透测试服务是模拟黑客攻击的方式，对业务系统的安全漏洞、安全隐患进行全面检测的安全服务。服务的最终目标是查找业务系统的安全漏洞、评估业务系统的安全状态，并提供相应的漏洞修复建议。	根据系统数量，按次计费	套	7800
	专业服务	资深专业人员驻场服务	资深网络和数据安全工程师具备深厚的技术背景和安全意识，能够持续跟踪和研究网络安全领域的最新动态和趋势，负责设计、开发和维护网络和数据安全系统，以确保组织的信息资产和数据安全。	1 人/月	1 人	16300	

	专业人员驻场服务	负责确保网络和数据安全的专业人员，涉及设计、实施和维护网络安全策略、安全架构以及安全系统，以预防、检测和应对网络安全威胁和数据泄露事件。	1人/月	1人	12800	
机柜托管	机柜服务	机柜租赁及服务器托管	机柜U数，按月计费	1U/月	200	

(二) 非xc云产品服务

主要为衢州市电子政务信息化系统提供所需非xc计算资源云计算服务。主要内容包含租赁服务主要包括如下基础云服务、中间件服务、安全服务、大数据服务等服务。

产品类别	产品子类	服务名称	计费方式	单位	最高限价 (元/月)	单项折扣 (%)
基础服务	云主机服务	云主机（含符合要求的操作系统）	根据核数，按月计费（vCPU主频>=2.2GHz）	core	36	
			根据内存，按月计费	GB	21.6	
		GPU服务器	14核56G，1×NVIDIA T4	1实例	1976	
			28核112G，2×NVIDIA T4	1实例	3290	
			40核160G，2×NVIDIA T4	1实例	4308	
			56核224G，4×NVIDIA T4	1实例	5318	
	块存储服务	高效云盘	根据存储容量，按月计费	GB	0.35	
		SSD云盘	根据存储容量，按月计费	GB	0.65	
		数据库存储	根据存储容量，按月计费	GB	0.7	
	对象存储服务	对象存储	根据存储容量，按月计费	GB	0.15	
	弹性IP	EIP	根据实例个数，按月计费	1实例	30	
负载均衡	负载均衡	根据实例个数，按月计费	1实例	40		
云数据库服务	RDS	通用型-MySQL	根据核数，按月计费	core	75	
			根据内存，按月计费	GB	40	
		独占型-MySQL	根据核数，按月计费	core	75	
			根据内存，按月计费	GB	52	
	RDS	MS SQL	根据核数，按月计费	core	66.4	
			根据内存，按月计费	GB	45.86	

	MongoDB	MongoDB	根据核数，按月计费	core	99.8	
			根据内存，按月计费	GB	68.8	
大数据服务	大数据服务	大数据计算服务	根据实例开通的 CU 数+存储容量(500G 起步)+增强软件包(非必选)，按月计费	实例开通 CU 数:	100	
				存储容量: GB	0.25	
	大数据开发治理平台	标准版	根据租户开通的版本按月收费，按套计费	租户	5000	
其他服务	云产品备份服务	ECS/RDS 快照服务	ECS/RDS 快照服务	TB	200	
	分布式应用服务	EDas 企业版	铂金版 (0-50) 实例	EDAS 租户	43000	
	主机托管	主机托管	根据 U 数，按月计费	1U	200	
安全服务	网络安全	漏洞扫描	根据云主机数量，按月计费	个	70	
		云堡垒机	根据云主机数量，按月计费	云主机	30	
		日志审计	根据日志源，按月计费	日志源	77	
		态势感知	根据受保护的云主机个数按月计算，默认按云主机一起开通	1 实例	48.1	
		安骑士	根据受保护的云主机个数按月计算，默认按云主机一起开通	1 实例	55.1	
		Web 应用防火墙	根据子域名数量，按月计费	子域名	200	
		零信任 (VPN 接入)	根据账户数量，按月计费	账户	35	
	渗透服务	渗透服务	根据系统数量，按次计费	套	7850	
	应用安全	代码审计	根据系统数量，按次计费	套	6000	
		主机安全防护	根据云主机数量，按月计费	个	60.8	
		高危隐患和安全事件预警	根据系统数量，按月计费	套	445.5	
		网络安全流量监测能力服务	根据系统数量，按月计费	套	445.5	
	数据安全	数据库权限管控系统	根据数据库实例，按月计费	1 实例	1195	
数据库审计		根据数据库实例，按月计费	1 实例	455		
静态脱敏		1/GB，按月计费	1/GB	7.87		

	数据备份	1/GB, 按月计费	1/GB	0.4	
	数据库监控平台服务	1 实例, 按月计费	1 实例	1000	
	数据库运维及安全评估报告	每月巡检报告, 1 次	1 次	600	
	数据库入侵防护 (云数据库防火墙)	根据数据库实例, 按月计费	1 实例	840	

注: 1. 单价报价不可超出最高单价限价。

2. 报价一经涂改, 应在涂改处加盖供应商公章或者由法定代表人或其授权代表签字或盖章, 否则其响应作无效标处理。

3. 本项目报价应包含人工费、交通费、餐费、材料费、税金、政策性风险和提供伴随服务等完成本项目的一切含税费用。如有合同费用漏项, 视同已包含在其项目中, 合同单价不作调整。

4. 以上数量为暂估数量, 最终根据实际数量及成交单价, 每年按实结算。

法定代表人或其授权代表: _____ (签字或盖章)

投标人名称: _____ (公章)

日期: _____ 年 _____ 月 _____ 日

采购活动现场确认声明书

衢州市开成工程造价咨询事务所有限公司：

本人经由_____（单位）负责人_____（姓名）合法授权参加衢州市政务云服务项目（编号：Qzkc2024-025）采购活动，经与本单位法人代表（负责人）联系确认，现就有关公平竞争事项郑重声明如下：

一、本单位与采购人之间 不存在利害关系 存在下列利害关系_____：

- A. 投资关系 B. 行政隶属关系 C. 业务指导关系
D. 其他可能影响采购公正的利害关系（如有，请如实说明）_____。

二、现已清楚知道参加本项目采购活动的其他所有供应商名称，本单位 与其他所有供应商之间均不存在利害关系 与_____（供应商名称）之间存在下列利害关系_____：

- A. 法定代表人或负责人或实际控制人是同一人
B. 法定代表人或负责人或实际控制人是夫妻关系
C. 法定代表人或负责人或实际控制人是直系血亲关系
D. 法定代表人或负责人或实际控制人存在三代以内旁系血亲关系
E. 法定代表人或负责人或实际控制人存在近姻亲关系
F. 法定代表人或负责人或实际控制人存在股份控制或实际控制关系
G. 存在共同直接或间接投资设立子公司、联营企业和合营企业情况
H. 存在分级代理或代销关系、同一生产制造商关系、管理关系、重要业务（占主营业务收入 50%以上）或重要财务往来关系（如融资）等其他实质性控制关系
I. 其他利害关系情况_____。

三、现已清楚知道并严格遵守采购法律法规和现场纪律。

四、我发现_____供应商之间存在或可能存在上述第二条第_____项利害关系。

授权代表签名：_____ 年 月 日

注：投标人在结束解密后 30 分钟内将填写完整且经授权代表签署的《采购活动现场确认声明书》扫描件发至经办人邮箱（邮箱地址：xueshilang@qzjrkg.com.cn）