**杭州市西湖区电子政务整体安全体系改造提升（2022）项目**

招标文件

 **（电子招投标）**

编号:XHZFCG-2022-G-42

杭州市西湖区数据资源管理局

杭州市西湖区政府采购中心

二〇二二年八月二十三日

**目 录**

第一部分 招标公告

第二部分 投标人须知

第三部分 采购需求

第四部分 评标办法

第五部分 拟签订的合同文本

第六部分 应提交的有关格式范例

**第一部分 招标公告**

项目概况

杭州市西湖区电子政务整体安全体系改造提升（2022）项目招标项目的潜在投标人应在政采云平台（[https://www.zcygov.cn/）获取（下载）招标文件，并于2022年9月13日09点30分00秒](https://www.zcygov.cn/%EF%BC%89%E8%8E%B7%E5%8F%96%EF%BC%88%E4%B8%8B%E8%BD%BD%EF%BC%89%E6%8B%9B%E6%A0%87%E6%96%87%E4%BB%B6%EF%BC%8C%E5%B9%B6%E4%BA%8E2021%E5%B9%B4)（北京时间）前递交（上传）投标文件。

**一、项目基本情况**

 **项目编号：**XHZFCG-2022-G-42

  **项目名称：**杭州市西湖区电子政务整体安全体系改造提升（2022）项目

  **预算金额（元）：** 6026000.00

**最高限价（元）：** 6026000.00

**采购需求：**杭州市西湖区电子政务整体安全体系改造提升（2022）项目,主要内容:更新网络边界、网络通信、计算环境等基础设施；搭建公共数据平台安全技术体系；升级迭代现有数据管控平台，实现全链路监管体系；完善攻防演练及应急处置服务、人员驻场服务（3名驻场人员）、网络重保服务等政府运营管理体系，主要包括硬件更新、软件升级开发、系统集成、系统培训，其中硬件质保期不少于3年，安全设备和机房设施维保服务不得少于1年，软件不少于1年（含）7×24小时免费售后技术服务。详见招标文件第三部分采购需求。

▲注：

1、本次投标总报价不得超过602.6万元整。

●更新网络边界、网络通信、计算环境等基础设施，搭建公共数据平台安全技术体系，升级迭代现有数据管控平台，实现全链路监管体系的报价不得超过546.6万元整；

●攻防演练及应急处置服务的报价不得超过6万元整/年，服务期3年；

●3名人员驻场服务的报价不得超过45万元整/年，服务期3年；

●网络重保支持服务的报价不得超过5万元整/年，服务期3年。

2、攻防演练及应急处置服务、人员驻场服务及网络重保支持服务的服务期均为3年，合同按年签定，每年验收合格后续签合同。

**合同履约期限：项目总建设工期3个月。**

**本项目接受联合体投标：**[x] **是，**[ ] **否**。

**二、申请人的资格要求：**

1. 满足《中华人民共和国政府采购法》第二十二条规定；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、政府采购严重违法失信行为记录名单；

 2. 以联合体形式投标的，提供联合协议(本项目不接受联合体投标或者投标人不以联合体形式投标的，则不需要提供) ；

3.落实政府采购政策需满足的资格要求：

[ ] 无（注：不得限制大中型企业与小微企业组成联合体参与投标）；

[x] 专门面向中小企业

[x] 服务全部由符合政策要求的中小企业承接，提供中小企业声明函；

[ ] 服务全部由符合政策要求的小微企业承接，提供中小企业声明函；

[ ] 要求以联合体形式参加，提供联合协议和中小企业声明函，联合协议中中小企业合同金额应当达到 %，小微企业合同金额应当达到 %;如果供应商本身提供所有标的均由中小企业制造、承建或承接，视同符合了资格条件，无需再与其他中小企业组成联合体参加政府采购活动，无需提供联合协议；

[ ] 要求合同分包，提供分包意向协议和中小企业声明函，分包意向协议中中小企业合同金额应当达到达到 % ，小微企业合同金额应当达到 % ;如果供应商本身提供所有标的均由中小企业制造、承建或承接，视同符合了资格条件，无需再向中小企业分包，无需提供分包意向协议；

4.本项目的特定资格要求：无；

5.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政府采购活动；为采购项目提供整体设计、规范编制或者项目管理、监理、检测等服务后不得再参加该采购项目的其他采购活动。

**三、获取招标文件**

**时间：**/至2022年9月13日，每天上午00:00至12:00 ，下午12:00至23:59（北京时间，线上获取法定节假日均可，线下获取文件法定节假日除外）

**地点（网址）：**政采云平台（https://www.zcygov.cn/）

**方式：**供应商登录政采云平台https://www.zcygov.cn/在线申请获取采购文件（进入“项目采购”应用，在获取采购文件菜单中选择项目，申请获取采购文件）。

**售价（元）：**0

**四、提交投标文件截止时间、开标时间和地点**

**提交投标文件截止时间：** 2022年9月13日09点 30分 （北京时间）

**投标地点（网址）：**政采云平台（https://www.zcygov.cn/）

**开标时间：**2022年9月13日 09点30 分

**开标地点（网址）：**政采云平台（https://www.zcygov.cn/）

**五、公告期限**

自本公告发布之日起5个工作日。

**六、其他补充事宜**

 1.《浙江省财政厅关于进一步发挥政府采购政策功能全力推动经济稳进提质的通知》 （浙财采监（2022）3号）、《浙江省财政厅关于进一步促进政府采购公平竞争打造最优营商环境的通知》（浙财采监（2021）22号）已分别于2022年1月29日和2022年2月1日开始实施，此前有关规定与上述文件内容不一致的，按上述文件要求执行。

 2.根据《浙江省财政厅关于进一步促进政府采购公平竞争打造最优营商环境的通知》（浙财采监（2021）22号）文件关于“健全行政裁决机制”要求，鼓励供应商在线提起询问，路径为：政采云-项目采购-询问质疑投诉-询问列表:鼓励供应商在线提起质疑，路径为：政采云-项目采购-询问质疑投诉-质疑列表。质疑供应商对在线质疑答复不满意的，可在线提起投诉，路径为：浙江政府服务网-政府采购投诉处理-在线办理。

3.供应商认为招标文件使自己的权益受到损害的，可以自获取招标文件之日或者招标文件公告期限届满之日（公告期限届满后获取招标文件的，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同级政府采购监督管理部门投诉。质疑函范本、投诉书范本请到浙江政府采购网下载专区下载。

4.其他事项：（1）需要落实的政府采购政策：包括节约资源、保护环境、支持创新、促进中小企业发展等。详见招标文件的第二部分总则。（2）电子招投标的说明：①电子招投标：本项目以数据电文形式，依托“政府采购云平台（www.zcygov.cn）”进行招投标活动，不接受纸质投标文件；②投标准备：注册账号--点击“商家入驻”，进行政府采购供应商资料填写；申领CA数字证书---申领流程详见“浙江政府采购网-下载专区-电子交易客户端-CA驱动和申领流程”；安装“政采云电子交易客户端”----前往“浙江政府采购网-下载专区-电子交易客户端”进行下载并安装；③招标文件的获取：使用账号登录或者使用CA登录政采云平台；进入“项目采购”应用，在获取采购文件菜单中选择项目，获取招标文件；④投标文件的制作：在“政采云电子交易客户端”中完成“填写基本信息”、“导入投标文件”、“标书关联”、“标书检查”、“电子签名”、“生成电子标书”等操作；⑤采购人、采购机构将依托政采云平台完成本项目的电子交易活动，平台不接受未按上述方式获取招标文件的供应商进行投标活动； ⑥对未按上述方式获取招标文件的供应商对该文件提出的质疑，采购人或采购代理机构将不予处理；⑦不提供招标文件纸质版；⑧投标文件的传输递交：投标人在投标截止时间前将加密的投标文件上传至政府采购云平台，还可以在投标截止时间前直接提交或者以邮政快递方式递交备份投标文件1份。备份投标文件的制作、存储、密封详见招标文件第二部分第15点—“备份投标文件”；⑨投标文件的解密：投标人按照平台提示和招标文件的规定在半小时内完成在线解密。通过“政府采购云平台”上传递交的投标文件无法按时解密，投标供应商递交了备份投标文件的，以备份投标文件为依据，否则视为投标文件撤回。通过“政府采购云平台”上传递交的投标文件已按时解密的，备份投标文件自动失效。投标人仅提交备份投标文件，未在电子交易平台传输递交投标文件的，投标无效；⑩具体操作指南：详见政采云平台“服务中心-帮助文档-项目采购-操作流程-电子招投标-政府采购项目电子交易管理操作指南-供应商”。（3）招标文件公告期限与招标公告的公告期限一致。

**七、对本次采购提出询问、质疑、投诉，请按以下方式联系**

 1.采购人信息

 名 称：杭州市西湖区数据资源管理局

 地 址：杭州市西湖区浙大路1号

传 真： /

项目联系人（询问）： 周奇倩

 项目联系方式（询问）：0571-87939232

 质疑联系人： 王泽恺

 质疑联系方式：0571-87939251

 2.采购代理机构信息

名 称：杭州市西湖区政府采购中心

地 址：杭州市文一西路858号

 传 真：0571-86834771

 项目联系人（询问）：江涛

 项目联系方式（询问）：0571-87759375

 质疑联系人：缪新新

 质疑联系方式：0571-85368157

 3.同级政府采购监督管理部门

 名 称：杭州市西湖区财政局政府采购监管科

 地 址：杭州市文三西路18号11楼1104

 传 真： /

 联系人 ：韩继伟

监督投诉电话：0571-58101865

若对项目采购电子交易系统操作有疑问，可登录政采云（https://www.zcygov.cn/），点击右侧咨询小采，获取采小蜜智能服务管家帮助，或拨打政采云服务热线400-881-7190获取热线服务帮助。

CA问题联系电话（人工）：汇信CA 400-888-4636；天谷CA 400-087-8198。

**第二部分 投标人须知**

**前附表**

| **序号** | **事项** | **本项目的特别规定** |
| --- | --- | --- |
| 1 | **项目属性** | 服务类。 |
| 2 | **采购标的及其对应的中小企业划分标准所属行业** | （1）标的： 系统升级改造 ，属于 软件和信息技术服务业 行业； |
| 3 | **是否允许采购进口产品** | [x] 本项目不允许采购进口产品。[ ] 可以就 采购进口产品。 |
| 4 | **分包** | [ ]  A同意将非主体、非关键性的 工作分包。[x]  B不同意分包。注：不得限制大中型企业向小微企业合理分包。 |
| 5 | **开标前答疑会或现场考察** | [x] A不组织。[ ] B组织，时间： ,地点： ，联系人： ，联系方式： 。 |
| 6 | **样品提供** | [x] A不要求提供。[ ] B要求提供，（1）样品： ；（2）样品制作的标准和要求： ；（3）样品的评审方法以及评审标准：详见评标办法；（4）是否需要随样品提交检测报告：[x] 否；[ ] 是，检测机构的要求： ；检测内容： 。（5）提供样品的时间： ；地点： ；联系人： ，联系电话： 。请投标人在上述时间内提供样品并按规定位置安装完毕。超过截止时间的，采购人或采购代理机构将不予接收，并将清场并封闭样品现场。 (6)采购活动结束后，对于未中标人提供的样品，采购人、采购机构将通知未中标人在规定的时间内取回，逾期未取回的，采购人、采购机构不负保管义务；对于中标人提供的样品，采购人将进行保管、封存，并作为履约验收的参考。（7）制作、运输、安装和保管样品所发生的一切费用由投标人自理。 |
| 7 | **方案讲解演示** | [ ] A不组织。[x] B组织。（1）在评标时安排每个投标人进行方案讲解演示。每个投标人时间不超过20分钟，**讲解次序以投标文件解密时间先后次序为准**，讲解演示人员不超过3人。讲解演示结束后按要求解答评标委员会提问。（2）方案讲解演示方式：通过政采云平台进行在线讲解演示**或**播放已录制好的演示视频（为确保视频播放过程中顺畅、不卡顿，播放视频的分辨率要求为1280\*720）。政采云平台在线讲解需投标人根据政采云平台操作要求做好准备工作，提前完善软硬件配置环境。注：因投标人自身原因导致无法演示或者演示效果不理想的，责任自负。因平台原因导致本项目方案讲解演示环节无法顺利开展，按照《浙江省政府采购项目电子交易管理暂行办法》相关规定执行。 |
| 8 | **投标人应当提供的资格、资信证明文件** | （1）资格证明文件：见招标文件第二部分11.1。投标人未提供有效的资格证明文件的，视为投标人不具备招标文件中规定的资格要求，投标无效。 |
| （2）资信证明文件：根据招标文件第四部分评标标准提供。 |
| 9 | **节能产品、环境标志产品** | 采购人拟采购的产品属于品目清单范围的，采购人及其委托的采购代理机构将依据国家确定的认证机构出具的、处于有效期之内的节能产品、环境标志产品认证证书，对获得证书的产品实施政府优先采购或强制采购。 |
| 10 | **报价要求** | 有关本项目实施所需的所有费用（含税费）均计入报价。开标一览表（报价表）是报价的唯一载体。投标文件中价格全部采用人民币报价。招标文件未列明，而投标人认为必需的费用也需列入报价。**提醒：验收时检测费用由采购人承担，不包含在投标总价中。****投标报价出现下列情形的，投标无效：****投标文件出现不是唯一的、有选择性投标报价的；****投标报价超过招标文件中规定的预算金额或者最高限价的;****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，未能按要求提供书面说明或者提交相关证明材料证明其报价合理性的;****投标人对根据修正原则修正后的报价不确认的。** |
| 11 | **中小企业信用融资** | 为支持和促进中小企业发展，进一步发挥政府采购政策功能，杭州市财政局与省银保监局、市地方金融监督管理局、市经信局共同出台了《杭州市政府采购支持中小企业信用融资管理办法》，供应商若有融资意向，详见《政府采购支持中小企业信用融资相关事项通知》，或登录杭州市政府采购网“中小企业信用融资”模块，查看信用融资政策文件及各相关银行服务方案。 |
| 供应商中标后也可在“政采云”平台申请政采贷：操作路径：登录政采云平台 - 金融服务中心 -【融资服务】，可在热门申请中选择产品直接申请，也可点击云智贷匹配适合产品进行申请，或者在可申请项目中根据该项目进行申请。 |
| 12 | **备份投标文件送达地点和签收人员**  | 备份投标文件送达地点：杭州市文一西路858号东3楼329办公室 ；备份投标文件签收人员联系电话： 0571-87759375。**采购人、采购机构不强制或变相强制投标人提交备份投标文件。** |
| 13 | **特别说明** | 联合体投标的或者以分包方式履行合同的，联合体各方（供应商与分包供应商）分别提供与联合体协议（分包意向协议）中规定的分工内容相应的业绩证明材料，业绩数量以提供材料较少的一方为准**。** |
| [ ] 联合体投标的，联合体各方均需按招标文件第四部分评标标准要求提供资信证明文件，否则视为不符合相关要求。[x] 联合体投标的，联合体中有一方或者联合体成员根据分工按招标文件第四部分评标标准要求提供资信证明文件的，视为符合了相关要求。 |

**一、总则**

**1. 适用范围**

本招标文件适用于该项目的招标、投标、开标、资格审查及信用信息查询、评标、定标、合同、验收等行为（法律、法规另有规定的，从其规定）。

 **2.定义**

2.1 “采购人”系指招标公告中载明的本项目的采购人。

2.2 “采购机构”系指招标公告中载明的本项目的采购机构。

2.3 “投标人”系指是指响应招标、参加投标竞争的法人、其他组织或者自然人。

2.4 “负责人”系指法人企业的法定负责人，或其他组织为法律、行政法规规定代表单位行使职权的主要负责人，或自然人本人。

2.5“电子签名”系指数据电文中以电子形式所含、所附用于识别签名人身份并表明签名人认可其中内容的数据；“公章”系指单位法定名称章。因特殊原因需要使用冠以法定名称的业务专用章的，投标时须提供《业务专用章使用说明函》（附件4）。

2.6“电子交易平台”是指本项目政府采购活动所依托的政府采购云平台（https://www.zcygov.cn/）。

2.7 “▲” 系指实质性要求条款，“[x] ” 系指适用本项目的要求，“[ ] ” 系指不适用本项目的要求。

**3.** **采购项目需要落实的政府采购政策**

3.1 本项目原则上采购本国生产的货物、工程和服务，不允许采购进口产品。除非采购人采购进口产品，已经在采购活动开始前向财政部门提出申请并获得财政部门审核同意，且在采购需求中明确规定可以采购进口产品（但如果因信息不对称等原因，仍有满足需求的国内产品要求参与采购竞争的，采购人、采购机构不会对其加以限制，仍将按照公平竞争原则实施采购）；优先采购向我国企业转让技术、与我国企业签订消化吸收再创新方案的供应商的进口产品。

3.2 支持绿色发展

3.2.1采购人拟采购的产品属于品目清单范围的，采购人及其委托的采购代理机构将依据国家确定的认证机构出具的、处于有效期之内的节能产品、环境标志产品认证证书，对获得证书的产品实施政府优先采购或强制采购。投标人须按招标文件要求提供相关产品认证证书。▲**采购人拟采购的产品属于政府强制采购的节能产品品目清单范围的，投标人未按招标文件要求提供国家确定的认证机构出具的、处于有效期之内的节能产品认证证书的，投标无效。**

3.2.2 修缮、装修类项目采购建材的，采购人应将绿色建筑和绿色建材性能、指标等作为实质性条件纳入招标文件和合同。

3.2.3为助力打好污染防治攻坚战，推广使用绿色包装，政府采购货物、工程和服务项目中涉及商品包装和快递包装的，供应商提供产品及相关快递服务的具体包装要求要参考《商品包装政府采购需求标准（试行）》、《快递包装政府采购需求标准（试行）》。优先采购绿色包装产品、绿色物流配送服务以及循环利用产品。

3.3支持中小企业发展

3.3.1中小企业，是指在中华人民共和国境内依法设立，依据国务院批准的中小企业划分标准确定的中型企业、小型企业和微型企业，但与大企业的负责人为同一人，或者与大企业存在直接控股、管理关系的除外。

符合中小企业划分标准的个体工商户，在政府采购活动中视同中小企业。

3.3.2在政府采购活动中，投标人提供的货物、工程或者服务符合下列情形的，享受中小企业扶持政策：在服务采购项目中，服务由中小企业承接，即提供服务的人员为中小企业依照《中华人民共和国劳动合同法》订立劳动合同的从业人员。

以联合体形式参加政府采购活动，联合体各方均为中小企业的，联合体视同中小企业。其中，联合体各方均为小微企业的，联合体视同小微企业。

3.3.3对于未预留份额专门面向中小企业的政府采购服务项目，以及预留份额政府采购服务项目中的非预留部分标项，对小型和微型企业的投标报价给予20%的扣除，用扣除后的价格参与评审。接受大中型企业与小微企业组成联合体或者允许大中型企业向一家或者多家小微企业分包的政府采购服务项目，对于联合协议或者分包意向协议约定小微企业的合同份额占到合同总金额30%以上的，对联合体或者大中型企业的报价给予6%的扣除，用扣除后的价格参加评审。组成联合体或者接受分包的小微企业与联合体内其他企业、分包企业之间存在直接控股、管理关系的，不享受价格扣除优惠政策。

3.3.4符合《关于促进残疾人就业政府采购政策的通知》（财库〔2017〕141号）规定的条件并提供《残疾人福利性单位声明函》（附件1）的残疾人福利性单位视同小型、微型企业；

3.3.5符合《关于政府采购支持监狱企业发展有关问题的通知》（财库[2014]68号）规定的监狱企业并提供由省级以上监狱管理局、戒毒管理局（含新疆生产建设兵团）出具的属于监狱企业证明文件的，视同为小型、微型企业。

3.3.6可享受中小企业扶持政策的投标人应按照招标文件格式要求提供《中小企业声明函》，投标人提供的《中小企业声明函》与实际情况不符的，不享受中小企业扶持政策。声明内容不实的，属于提供虚假材料谋取中标、成交的，依法承担法律责任。

3.3.7中小企业享受扶持政策获得政府采购合同的，小微企业不得将合同分包给大中型企业，中型企业不得将合同分包给大型企业。

3.4支持创新发展

3.4.1 采购人优先采购被认定为首台套产品和“制造精品”的自主创新产品。

3.4.2首台套产品被纳入《首台套产品推广应用指导目录》之日起3年内，以及产品核心技术高于国内领先水平，并具有明晰自主知识产权的“制造精品”产品，自认定之日起2年内视同已具备相应销售业绩，参加政府采购活动时业绩分值为满分。

3.5中小企业信用融资：为支持和促进中小企业发展，进一步发挥政府采购政策功能，杭州市财政局与省银保监局、市金融办、市经信局共同出台了《杭州市政府采购支持中小企业信用融资管理办法》，供应商若有融资意向，详见《政府采购支持中小企业信用融资相关事项通知》，或登录杭州市政府采购网“中小企业信用融资”模块，查看信用融资政策文件及各相关银行服务方案。

3.5平等对待内外资企业和符合条件的破产重整企业

平等对待内外资企业和符合条件的破产重整企业，切实保障企业公平竞争，平等维护企业的合法利益。**4. 询问、质疑、投诉**

4.1供应商询问

供应商对政府采购活动事项有疑问的，可以提出询问，采购人或者采购代理机构应当在3个工作日内对供应商依法提出的询问作出答复，但答复的内容不得涉及商业秘密。供应商提出的询问超出采购人对采购代理机构委托授权范围的，采购代理机构应当告知供应商向采购人提出。

4.2供应商质疑

4.2.1提出质疑的供应商应当是参与所质疑项目采购活动的供应商。潜在供应商已依法获取其可质疑的招标文件的，可以对该文件提出质疑。

4.2.2供应商认为招标文件、采购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七个工作日内，以书面形式向采购人或者采购机构提出质疑，否则，采购人或者采购机构不予受理：

4.2.2.1对招标文件提出质疑的，质疑期限为供应商获得招标文件之日或者招标文件公告期限届满之日起计算。

4.2.2.2对采购过程提出质疑的，质疑期限为各采购程序环节结束之日起计算。4.2.2.3对采购结果提出质疑的，质疑期限自采购结果公告期限届满之日起计算。

4.2.3供应商提出质疑应当提交质疑函和必要的证明材料。质疑函应当包括下列内容：

　　4.2.3.1供应商的姓名或者名称、地址、邮编、联系人及联系电话；

　　4.2.3.2质疑项目的名称、编号；

　　4.2.3.3具体、明确的质疑事项和与质疑事项相关的请求；

　　4.2.3.4事实依据；

　　4.2.3.5必要的法律依据；

4.2.3.6提出质疑的日期。

供应商提交的质疑函需一式三份。供应商为自然人的，应当由本人签字；供应商为法人或者其他组织的，应当由法定代表人、主要负责人，或者其授权代表签字或者盖章，并加盖公章。

质疑函范本及制作说明详见附件2。

4.2.4对同一采购程序环节的质疑，供应商须在法定质疑期内一次性提出。

4.2.5采购人或者采购机构应当在收到供应商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供应商和其他与质疑处理结果有利害关系的政府采购当事人，但答复的内容不得涉及商业秘密。根据《杭州市财政局关于进一步加强政府采购信息公开优化营商环境的通知》（杭财采监〔2021〕17号）,采购人或者采购机构在质疑回复后5个工作日内，在浙江政府采购网的“其他公告”栏目公开质疑答复，答复内容应当完整。质疑函作为附件上传。

4.2.6询问或者质疑事项可能影响采购结果的，采购人应当暂停签订合同，已经签订合同的，应当中止履行合同。

4.3供应商投诉

4.3.1质疑供应商对采购人、采购机构的答复不满意或者采购人、采购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同级政府采购监督管理部门提出投诉。

4.3.2供应商投诉的事项不得超出已质疑事项的范围，基于质疑答复内容提出的投诉事项除外。

4.3.3供应商投诉应当有明确的请求和必要的证明材料。

4.3.5 以联合体形式参加政府采购活动的，其投诉应当由组成联合体的所有供应商共同提出。

投诉书范本及制作说明详见附件3。

4.4在线质疑、投诉。

根据《浙江省财政厅关于进一步促进政府采购公平竞争打造最优营商环境的通知》（浙财采监（2021）22号）文件关于“健全行政裁决机制”要求，鼓励供应商在线提起询问，路径为：政采云-项目采购-询问质疑投诉-询问列表；鼓励供应商在线提起质疑，路径为：政采云-项目采购-询问质疑投诉-质疑列表。质疑供应商对在线质疑答复不满意的，可在线提起投诉，路径为：浙江政府服务网-政府采购投诉处理-在线办理。

 **二、招标文件的构成、澄清、修改**

**5．招标文件的构成**

5.1 招标文件包括下列文件及附件：

5.1.1招标公告；

5.1.2投标人须知；

5.1.3采购需求；

5.1.4评标办法；

5.1.5拟签订的合同文本；

5.1.6应提交的有关格式范例。

5.2与本项目有关的澄清或者修改的内容为招标文件的组成部分。

**6. 招标文件的澄清、修改**

6.1已获取招标文件的潜在投标人，若有问题需要澄清，应于投标截止时间前，以书面形式向采购机构提出。

6.2 采购机构对招标文件进行澄清或修改的，将同时通过电子交易平台通知已获取招标文件的潜在投标人。依法应当公告的，将按规定公告，同时视情况延长投标截止时间和开标时间。该澄清或者修改的内容为招标文件的组成部分。

**三、投标**

**7. 招标文件的获取**

详见招标公告中获取招标文件的时间期限、地点、方式及招标文件售价。

**8.开标前答疑会或现场考察**

采购人组织潜在投标人现场考察或者召开开标前答疑会的，潜在投标人按第二部分投标人须知前附表的规定参加现场考察或者开标前答疑会。

**9.投标保证金**

本项目不需缴纳投标保证金。

**10. 投标文件的语言**

投标文件及投标人与采购有关的来往通知、函件和文件均应使用中文。

**11. 投标文件的组成**

11.1**资格文件**：

11.1.1符合参加政府采购活动应当具备的一般条件的承诺函；

11.1.2联合协议（如果有)；

11.1.3落实政府采购政策需满足的资格要求（如果有）；

11.1.4本项目的特定资格要求（如果有)。

11.2 商务技术文件：

11.2.1投标函；

11.2.2授权委托书或法定代表人（单位负责人、自然人本人）身份证明；

11.2.3分包意向协议（如果有)；

11.2.4符合性审查资料；

11.2.5评标标准相应的商务技术资料；

11.2.6 投标标的清单；

11.2.7商务技术偏离表；

11.2.8政府采购供应商廉洁自律承诺书；

11.3**报价文件：**

11.3.1开标一览表（报价表）。

**投标文件含有采购人不能接受的附加条件的，投标无效；**

**投标人提供虚假材料投标的，投标无效。**

**12. 投标文件的编制**

12.1投标文件分为资格文件、商务技术文件、报价文件三部分。各投标人在编制投标文件时请按照招标文件第六部分规定的格式进行，混乱的编排导致投标文件被误读或评标委员会查找不到有效文件是投标人的风险。

12.2投标人进行电子投标应安装客户端软件—“政采云电子交易客户端”，并按照招标文件和电子交易平台的要求编制并加密投标文件。投标人未按规定加密的投标文件，电子交易平台将拒收并提示。

12.3使用“政采云电子交易客户端”需要提前申领CA数字证书，申领流程请自行前往“浙江政府采购网-下载专区-电子交易客户端-CA驱动和申领流程”进行查阅。

**13.投标文件的签署、盖章**

13.1投标文件按照招标文件第六部分格式要求进行签署、盖章。**▲投标人的投标文件未按照招标文件要求签署、盖章的，其投标无效**。

13.2为确保网上操作合法、有效和安全，投标人应当在投标截止时间前完成在“政府采购云平台”的身份认证，确保在电子投标过程中能够对相关数据电文进行加密和使用电子签名。

13.3招标文件对投标文件签署、盖章的要求适用于电子签名。

**14. 投标文件的提交、补充、修改、撤回**

14.1 供应商应当在投标截止时间前完成投标文件的传输递交，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、修改后重新传输递交。投标截止时间前未完成传输的，视为撤回投标文件。投标截止时间后递交的投标文件，电子交易平台将拒收。

14.2电子交易平台收到投标文件，将妥善保存并即时向供应商发出确认回执通知。在投标截止时间前，除供应商补充、修改或者撤回投标文件外，任何单位和个人不得解密或提取投标文件。

14.3采购人、采购机构可以视情况延长投标文件提交的截止时间。在上述情况下，采购机构与投标人以前在投标截止期方面的全部权利、责任和义务，将适用于延长至新的投标截止期。

**15.备份投标文件**

 15.1投标人在电子交易平台传输递交投标文件后，还可以在投标截止时间前直接提交或者以邮政快递方式递交备份投标文件1份，**但采购人、采购机构不强制或变相强制投标人提交备份投标文件。**

15.2备份投标文件须在“政采云投标客户端”制作生成，并储存在DVD光盘中。备份投标文件应当密封包装并在包装上加盖公章并注明投标项目名称，投标人名称(联合体投标的，包装物封面需注明联合体投标，并注明联合体成员各方的名称和联合协议中约定的牵头人的名称)。**不符合上述制作、存储、密封规定的备份投标文件将被视为无效或者被拒绝接收。**

15.3直接提交备份投标文件的，投标人应于投标截止时间前在招标公告中载明的开标地点将备份投标文件提交给采购机构，采购机构将拒绝接受逾期送达的备份投标文件。

15.4以邮政快递方式递交备份投标文件的，投标人应先将备份投标文件按要求密封和标记，再进行邮政快递包装后邮寄。备份投标文件须在投标截止时间之前送达招标文件第二部分投标人须知前附表规定的备份投标文件送达地点；送达时间以签收人签收时间为准。采购机构将拒绝接受逾期送达的备份投标文件。邮寄过程中，电子备份投标文件发生泄露、遗失、损坏或延期送达等情况的，由投标人自行负责。

**15.5投标人仅提交备份投标文件，未在电子交易平台传输递交投标文件的，投标无效。**

**16.投标文件的无效处理**

有招标文件第四部分4.2规定的情形之一的，投标无效：

**17.投标有效期**

17.1投标有效期为从提交投标文件的截止之日起90天。▲**投标人的投标文件中承诺的投标有效期少于招标文件中载明的投标有效期的，投标无效。**

17.2投标文件合格投递后，自投标截止日期起，在投标有效期内有效。

17.3在原定投标有效期满之前，如果出现特殊情况，采购机构可以以书面形式通知投标人延长投标有效期。投标人同意延长的，不得要求或被允许修改其投标文件，投标人拒绝延长的，其投标无效。

**四、开标、资格审查与信用信息查询**

**18.开标**

18.1 采购机构按照招标文件规定的时间通过电子交易平台组织开标，所有投标人均应当准时在线参加。投标人不足3家的，不得开标。

　18.2 开标时，电子交易平台按开标时间自动提取所有投标文件。采购机构依托电子交易平台发起开始解密指令，投标人按照平台提示和招标文件的规定在半小时内完成在线解密。

　18.3 **投标文件未按时解密，投标人提供了备份投标文件的，以备份投标文件作为依据，否则视为投标文件撤回。投标文件已按时解密的，备份投标文件自动失效。**

**19、资格审查**

19.1开标后，采购人或采购机构将依法对投标人的资格进行审查。

19.2采购人或采购机构依据法律法规和招标文件的规定，对投标人的资格进行审查。

19.3投标人未按照招标文件要求提供与资格条件相应的有效资格证明材料的，视为投标人不具备招标文件中规定的资格要求，其投标无效。

19.4对未通过资格审查的投标人，采购人或采购机构告知其未通过的原因。

19.5合格投标人不足3家的，不再评标。

**20、信用信息查询**

20.1信用信息查询渠道及截止时间：采购机构将在资格审查时通过“信用中国”网站(www.creditchina.gov.cn)、中国政府采购网(www.ccgp.gov.cn)渠道查询投标人接受资格时的信用记录。

20.2信用信息查询记录和证据留存的具体方式：现场查询的投标人的信用记录、查询结果经确认后将与采购文件一起存档。

20.3信用信息的使用规则：经查询列入失信被执行人名单、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将被拒绝参与政府采购活动。

20.4联合体信用信息查询：两个以上的自然人、法人或者其他组织组成一个联合体，以一个供应商的身份共同参加政府采购活动的，应当对所有联合体成员进行信用记录查询，联合体成员存在不良信用记录的，视同联合体存在不良信用记录。

**五、评标**

**21.** 评标委员会将根据招标文件和有关规定，履行评标工作职责，并按照评标方法及评分标准，全面衡量各投标人对招标文件的响应情况。对实质上响应招标文件的投标人，按照评审因素的量化指标排出推荐中标的投标人的先后顺序，并按顺序提出授标建议。**详见招标文件第四部分评标办法。**

**六、定 标**

**22. 确定中标供应商**

政府采购项目实行全流程电子化，评审报告送交、采购结果确定和结果公告均在线完成。为进一步提升采购结果确定效率，采购代理机构应当依法及时将评审报告在线送交采购人。采购单位应当自收到评审报告之日起2个工作日内在线确定中标或者成交供应商。中标、成交通知书和中标、成交结果公告应当在规定时间内同时发出。

**23. 中标通知与中标结果公告**

23.1自中标人确定之日起2个工作日内，采购机构通过电子交易平台向中标人发出中标通知书，同时编制发布采购结果公告。采购机构也可以以纸质形式进行中标通知。

23.2中标结果公告内容包括采购人及其委托的采购机构的名称、地址、联系方式，项目名称和项目编号，中标人名称、地址和中标金额，主要中标标的的名称、规格型号、数量、单价、服务要求，开标记录、**资格审查情况、评审专家抽取规则、符合性审查情况、**未中标情况说明、中标公告期限以及评审专家名单、评分汇总及明细。

23.3公告期限为1个工作日。

**七、合同授予**

**24.** 合同主要条款详见第五部分拟签订的合同文本。

**25. 合同的签订**

25.1 采购人与中标人应当通过电子交易平台在中标通知书发出之日起三十日内，按照招标文件确定的事项签订政府采购合同，并在签订之日起2个工作日内将政府采购合同在浙江政府采购网上公告。鼓励有条件的采购人视情缩减采购合同签订时限，提高采购效率，杜绝“冷、硬、横、推”等不当行为。除不可抗力等特殊情况外，原则上应当在中标通知书发出之日起10个工作日内，与中标供应商按照采购文件确定的事项签订政府采购合同。

25.2中标人按规定的日期、时间、地点，由法定代表人或其授权代表与采购人代表签订合同。如中标人为联合体的，由联合体成员各方法定代表人或其授权代表与采购人代表签订合同。

25.3如签订合同并生效后，供应商无故拒绝或延期，除按照合同条款处理外，列入不良行为记录一次，并给予通报。

25.4中标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中标或者成交候选人名单排序，确定下一候选人为中标供应商，也可以重新开展政府采购活动。

25.5采购合同由采购人与中标供应商根据招标文件、投标文件等内容通过政府采购电子交易平台在线签订，自动备案。

**26. 履约保证金**

拟签订的合同文本要求中标供应商提交履约保证金的，供应商应当以支票、汇票、本票或者金融机构、担保机构出具的保函等非现金形式提交。履约保证金的数额不得超过政府采购合同金额的1%。鼓励和支持供应商以银行、保险公司出具的保函形式提供履约保证金。采购人不得拒收履约保函，项目验收结束后应及时退还，延迟退还的，应当按照合同约定和法律规定承担相应的赔偿责任。

政府采购货物和服务项目中，采购单位可根据杭州市政府采购网公布的供应商履约评价情况减免履约保证金。供应商履约验收评价总分为100分的，采购单位应当免收履约保证金。

## 供应商可登录政采云平台-【金融服务】—【我的项目】—【已备案合同】以保函形式提供：1、供应商在合同列表选择需要投保的合同，点击[保函推荐]。2、在弹框里查看推荐的保函产品，供应商自行选择保函产品，点击[立即申请]。3、在弹框里填写保函申请信息。具体步骤：选择产品—填写供应商信息—选择中标项目—确认信息—等待保险/保函受理—确认保单—支付保费—成功出单。政采云金融专线400-903-9583。

**八、电子交易活动的中止**

2**7. 电子交易活动的中止。**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，采购机构可中止电子交易活动：

27.1电子交易平台发生故障而无法登录访问的；

27.2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；

27.3电子交易平台发现严重安全漏洞，有潜在泄密危险的；

27.4病毒发作导致不能进行正常操作的；

27.5其他无法保证电子交易的公平、公正和安全的情况。

 28.出现以上情形，不影响采购公平、公正性的，采购组织机构可以待上述情形消除后继续组织电子交易活动，也可以决定某些环节以纸质形式进行；影响或可能影响采购公平、公正性的，应当重新采购。

**九、验收**

**29.验收**

29.1采购人组织对供应商履约的验收。大型或者复杂的政府采购项目，应当邀请国家认可的质量检测机构参加验收工作。验收方成员应当在验收书上签字，并承担相应的法律责任。如果发现与合同中要求不符，供应商须承担由此发生的一切损失和费用，并接受相应的处理。

29.2采购人可以邀请参加本项目的其他投标人或者第三方机构参与验收。参与验收的投标人或者第三方机构的意见作为验收书的参考资料一并存档。

29.3严格按照采购合同开展履约验收。采购人成立验收小组，按照采购合同的约定对供应商履约情况进行验收。验收时，按照采购合同的约定对每一项技术、服务、安全标准的履约情况进行确认。验收结束后，应当出具验收书，列明各项标准的验收情况及项目总体评价，由验收双方共同签署。验收结果与采购合同约定的资金支付及履约保证金返还条件挂钩。履约验收的各项资料应当存档备查。

29.4验收合格的项目，采购人将根据采购合同的约定及时向供应商支付采购资金、退还履约保证金。验收不合格的项目，采购人将依法及时处理。采购合同的履行、违约责任和解决争议的方式等适用《中华人民共和国民法典》。供应商在履约过程中有政府采购法律法规规定的违法违规情形的，采购人应当及时报告本级财政部门。

**第三部分 采购需求**

**一、项目概述**

将数字化贯穿到西湖区电子政务安全的全过程各方面，统筹推进数字技术应用和制度创新，以一体化智能化公共数据平台安全为核心，参照国家法律法规、标准规范和省市文件要求，从安全管理体系、安全技术体系、安全运营体系等维度，加强全区政务网络、政务应用、政务数据基础设施安全；完善政务数据全生命周期安全，建立和提升覆盖云、网端、边界、应用、数据的一体化全链路网络安全监管体系；建立健全全区政务网络、政务应用和政务数据安全检测评估和安全运营体系，为“数字化改革”推进提供全方位安全保障。

**二、建设内容**

 项目建设内容包括以下：

**1、加强电子政务平台基础安全防护**

根据《中华人民共和国网络安全法》、《等保2.0》、《县级公共数据平台建设导则》等相关要求，按照网络安全等级保护三级标准对网络边界、网络通信、计算环境等基础设施进行完善。

**2、建立公共数据平台安全技术体系**

参考《县级公共数据平台建设导则》，结合西湖区一体化智能化公共数据平台建设，围绕公共数据平台数据采集、传输、存储、处理、交换、销毁等环节的数据安全保密需求，形成公共数据平台安全技术体系。

**3、建立政务外网全链路安全监管体系**

结合全省全链路安全监管要求，在现有的数据管控平台基础上进行升级迭代，构建覆盖云、网、端、边界、应用、数据的全链路监管体系。

**4、强化电子政务安全评估检测和运营管理**

强化政务网络安全评估、等保三级系统密码应用测评，完善网络重保、攻防演练、运行维护等政务运营管理体系。

**三、项目采购清单**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 序号 | 设备清单 | 配置简要描述 | 单位 | 数量 |
| 1 | 日志审计系统 | 2U机架式，内存容量：≧32GB\*4， 10块4T硬盘，4个千兆电口，2个万兆光口；资产授权许可数量：≧1000个。**三年免费质保及技术支持服务。** | 台 | 1 |
| 2 | 终端安全软件 | 终端安全软件，实现政务外网终端的病毒查杀、补丁分发以及终端管控。许可数量：3000节点。**两年免费质保及病毒库更新**。 | 项 | 1 |
| 3 | 端点检测和响应系统（EDR） | 端点检测和响应系统（EDR），含管理平台一套及不少于450节点授权。**三年免费质保及技术支持服务。** | 套 | 1 |
| 4 | 威胁狩猎与溯源系统 | 2U机架式，内存≧32G，2个千兆网卡，双电源，配置4个沙箱，16个代理，包含沙箱仿真模块、伪装代理模块、攻击溯源模块、诱导感知模块、系统管理模块等。**三年免费质保及技术服务。** | 台 | 1 |
| 5 | 代码审计系统 | 2U机架式，内存≧128G，存储≧4TB，双电源，支持对C、C++、C#、Objective-C、Java、PHP、Swift、JavaScript、Python、Cobol、Go等语言开发的软件源代码进行安全缺陷检测；支持软件版本管理系统集成；能够从这些软件版本管理系统发起源代码安全缺陷检测任务。**三年免费质保及技术服务。** | 台 | 1 |
| 6 | 数据库加密系统 | 2U机架式，双电源，2GE板载管理口，4GE板载接口，1×接口板卡插槽。≧16GB内存，≧2TB硬盘。支持Oracle，MySQL，Microsoft SQL Server等数据库类型。配置10个数据库(IP+Port)授权。**三年免费质保及技术服务。** | 台 | 2 |
| 7 | 数据库权限管控系统 | 2U机架式，双电源，≧6个千兆电口，≧16G内存，≧2T存储空间，配置16个数据库实例授权，支持采用身份管理、授权等机制对数据库运维操作进行合规管理。**三年免费质保及技术服务。** | 台 | 1 |
| 8 | 数据库脱敏系统 | 支持常用数据库：MySQL、Oracle、PostgreSQL、MSSQL、MariaDB、GreenPlum、DB2、Informix等。**三年免费质保及技术服务。** | 套 | 1 |
| 9 | 数据水印系统 | 配置数据库管理授权5个，支持Oracle、SQLServer、Mysql、PostgreSQL、ODPS等主流数据库。**三年免费质保及技术服务。** | 套 | 1 |
| 10 | 数据安全管控分析服务 | 基于现有数据管控平台，扩展数据安全管控能力，实现业务场景梳理、场景大屏定制、共享与回流防护、安全检查平台运营等服务。**服务期：1年。** | 项 | 1 |
| 11 | 全链路安全监管升级服务 | 在现有数据管控平台进行升级，增加监测范围，升级监测力度，增加云、网络及边界、应用、终端方面的安全监测能力，含资产管理升级服务、告警管理升级服务、通报处置升级服务、监督检查升级服务、知识库管理升级服务、考核评估升级服务、态势感知升级服务、事件案例升级服务。**服务期：1年。** | 项 | 1 |
| 12 | 风险评估服务 | 依据省、市数据安全检查的要求，对10个重要业务系统进行风险评估，包括漏洞扫描（每年4次）、安全基线检查（每年4次）、渗透测试（每年1次）、出具《漏洞扫描报告》（4份）、《安全基线检查报告》（4份）、《渗透测试报告》（1份）、《风险评估报告》（1份）。**服务期1年。** | 项 | 1 |
| 13 | 密码应用测评 | 依据《信息系统密码应用基本要求》，对5个网络安全等保三级及以上政务信息系统开展国产密码应用评估。 | 项 | 1 |
| 14 | 攻防演练及应急处置服务 | 制定应急预案，并根据实际演练情况对应急预案的有效性、落地性进行检验，对重要信息系统的防御措施进行检查与评估，发现风险。服务期内如遇安全事件，及时协助客户进行应急响应处置，追踪溯源。**每年提供1次服务。** | 年 | 3 |
| 15 | 人员驻场服务 | 3人常驻现场服务，提供5×8小时现场技术服务。服务内容：1、网络安全技术支持服务：安全设备运维管理和日常巡检、网络安全事件处置和通报、协调安全加固等；2、数据安全技术支持服务：配合区数据资源局完成政务数据安全技术和管理措施落实工作，包括安全自查、部门安全检查、数据安全设施操作使用和日常维护、相关制度规范文档和工作台账整理等；3、终端及外设日常故障处理；4、用户交办的其他工作。具体工作由业主根据实际需要安排。 | 年 | 3 |
| 16 | 网络重保支持服务 | 重要会议、重大活动、重要事件期间，委派资深安服技术人员到场，为电子政务网络、安全、云计算平台等设备正常稳定运行提供保障，随时应急处理全区电子政务网络突发故障。人员须具备至少3年以上网络技术工作经验，服务时长：每年不少于27人天。 | 年 | 3 |
| 17 | 设备维保服务 | 天融信TSC-71232-WVS漏洞扫描系统一台；安恒DAS-A1000数据库审计设备一台；深信服SIP-1000－A600态势感知平台一套。**服务期：1年** | 项 | 1 |

**四、采购内容及详细招标参数要求**(指标及要求所述的“支持”内容均包含在此次采购项目中)

**1、日志审计系统**

|  |  |
| --- | --- |
| **技术指标** | **技术规格要求** |
| 硬件规格 | ≧4个千兆电口，≧2个万兆光口； |
| 内存≧32GB\*4，磁盘≧4T\*10； |
| 处理性能 | 峰值处理能力EPS≧20000/秒(峰值30000/秒)； |
| 功能扩展 | 支持手动或按周期自动备份系统配置，可随时对系统资产等配置进行还原操作，且自动备份周期与备份包个数可配；支持系统配置备份自动备份至远程服务器； |
| ★支持kafka日志接收转发、大数据安全域同步、沙箱报告转发等大数据联调功能；**（提供截图证明)** |
| 日志收集 | 支持Syslog、SNMP Trap、HTTP、ODBC/JDBC、WMI、FTP、SFTP协议日志收集；支持阿里云SLS日志的采集； |
| 设备厂家包括但不限于：Cisco(思科)、Juniper、联想网御/网御神州、F5、华为、H3C、微软、绿盟、飞塔(Fortinet)、Foundry、天融信、启明星辰、天网、趋势、东软、Nokia、CheckPoint、Hillstone(山石)、安恒信息、珠海伟思、BEA、中国电信、安氏、帕拉迪、APC、Arbor、Clam、戴尔（Dell）、Digium、东方电子、EMC、中国电力科学研究院、Eudora、Google、冠群金辰、Linksys、McAFee、Netapp、永达、Sonicwall、Vigor、天存、Symantec（赛门铁克）、Hardened-PHP、Foundertech(方正)、三零盛安、Allot、蓝盾、IBM、金诺网安、网威、Nortel(北电)、Citrix(思杰)、Watchguard、中兴、阿帕奇、Windows系统日志、Linux/UNIX syslog、IIS、Apache等； |
| 支持常见的虚拟机环境日志收集，包括Xen、VMWare、Hyper-V等； |
| 支持目前主流的网络安全设备、交换设备、路由设备、操作系统、应用系统等； |
| 日志分析 | 支持对收集到的重复日志进行自动聚合归并，减少日志量； |
| 支持将收集到的日志转发，当原始日志设备无法设置多个日志服务器时，可以通过本系统的日志转发功能将日志转发到其他日志存储设备； |
| 内置5000+解析规则，支持对收集的5000+设备类型日志进行解析（标准化、归一化），解析维度多达200+，解析规则可以根据客户要求定制扩展； |
| ★三维关联分析；支持通过资产、安全知识库、弱点库三个维度分析事件是否存在威胁，并形成关联事件；**（提供第三方检测报告）** |
| 综合查询及报表管理 | 内置合规性报表1000+种； |
| 支持报表导出为PDF和Word格式文件； |
| 日志备份 | 支持日志备份自动传送到远程服务器； |
| 支持从远程仓库恢复数据； |
| 告警功能 | 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；资产性能监控异常告警，对于监控的资产系统资源进行监测当指定指标使用率达到设定的阈值时可产生并外发告警；资产状态监控，当资产处于不活跃状态时可产生并外发告警；远程仓库状态监测可告警，当远程仓库可用性检测失败或备份包自动上传失败时可产生并外发告警；**（提供截图证明）** |
| 具备报警合并和在一个时间段内抑制报警次数的能力； |
| 应用性能监控 | ★通过在目标主机上安装Agent程序，支持监测目标主机的CPU利用率、内存使用率、磁盘使用率、磁盘使用情况、流量等信息；**（提供第三方检测报告）** |
| 支持监控MySQL以下参数：查询缓存命中率、键缓存命中率、立即获得锁数、连接数、线程数、每秒SQL查询数、每秒发送字节、每秒接收字节； |
| 用户管理 | 用户支持双因子认证登录，双因子认证令牌支持绑定至具体用户；**（提供截图证明）** |
| 提供自助式的升级接口，支持对产品升级、规则升级； |
| 资产管理 | 注册用户资产时，提供自动发现识别能力； |
| 资产拓扑支持按照实际的用户环境进行编辑发布并可以和资产进行绑定，扑可以显示资产采集的事件数量被采集资产的状态等信息；**（提供第三方检测报告）** |
| 服务要求 | 三年免费质保。 |

**2、终端安全软件**

|  |  |
| --- | --- |
| **技术指标** | **技术规格要求** |
| 产品形态 | 软件形态，包含管理控制中心、客户端软件，本次授权许可数量：3000 |
| 控制中心要求 | 控制中心支持单机部署和集群部署两种方式，控制中心根据客户端点数的增加支持横向扩展；操作系统支持Windows Server 2012/2012 R2/2016的64位版本（简体中文版）；支持CentOS 7系统； |
| 控制中心支持安装在虚拟机上； |
| 控制中心支持级联管理，可支持5级级联部署，亦可单机和集群部署混合级联； |
| 客户端要求 | 操作系统：Windows XP\_SP3及以上/Windows Vista/Windows 7/Windows10；Windows Server 2008/Windows Server 2012/Windows Server 2016/Windows Server 2019；macOS X 10.11/macOS X 10.12/macOS X 10.13/macOS X 10.14/macOS X 10.15/macOS X 10.16/macOS X 11.0；CentOS 5~8/Red Hat Enterprise Linux 5~8； |
| 终端许可管理 | 支持按照终端类型/分组统计及分配管理每个功能的终端授权使用数量。 |
| 控制中心管理 | 支持控制中心迁移、数据备份、数据恢复；支持多升级服务器； |
| 支持根据分组、计算机名称、IP地址、操作系统、在线状态等条件的组合筛选出符合条件的终端进行管理； |
| 支持单个页面展示终端部署统计、终端安全趋势、终端状态（文件防护开启率、未安装补丁终端率、终端病毒更新率和终端版本更新率）、终端程序版本、终端在线统计、病毒库版本分布、安全更新和重要补丁安全趋势等信息，均可通过图形化展示； |
| 支持定时公告功能，可配置开机显示、周期显示和立即推送； |
| 支持对单个客户端进行维护，终端视角查看终端基本信息，包括计算机名、型号、IP、MAC地址、工作组、域信息、本次开机时间、上次关机时间、应用功能、在线状态；所功能应用策略情况；硬件信息展示，包括CPU、主板、内存、磁盘存储、显卡、显示器、声卡、网卡等信息；实时进程信息展示，包括进程名称、PID、进程用户名、命令行、占用内存、CPU占用、MD5等信息；网络信息展示，包括IP获取方式、IP地址、子网掩码、默认网关、DNS等信息； |
| 管理控制中心当登录账号输入密码错误次数超过锁定阈值后账号将被锁定，且可设置锁定时间，该时间内账号登录请求不被接受。同时应支持双因子认证登录方式，提高安全性； |
| 支持定义不同权限管理员角色，通过角色能够对有相同权限需求的用户进行授权，达到复用的能力；而对于没有复用的权限，可通过基于规则方式进行授权，支持角色层级管理，可至少达到5级新建角色。简化管理员对角色的管理成本，提高效率； |
| 客户端管理 | 支持终端密码保护功能，支持终端“防退出”密码保护、“防卸载”密码保护、防安装密码保护。支持设置自我保护功能，可有效防止客户端进程被恶意终止、注入、提高客户端进程、数据、配置的安全性； |
| 支持自定义定制客户端标题、皮肤、语言、产品LOGO、企业LOGO、认证弹窗LOGO； |
| 病毒防护概况 | 病毒防护概况：终端基础信息、病毒库版本、发现病毒数、未处理病毒数、最后查杀时间、文件防护状态、引擎使用状态、扩展病毒库版本； |
| 病毒查杀日志 | 病毒防护日志包含：病毒查杀日志、查杀任务日志、攻击防护日志、系统防护日志、按分组、按终端、按时间； |
| 病毒防护报表 | 病毒报表支持病毒查杀趋势、扫描触发方式趋势、发现病毒趋势、终端感染趋势、病毒类型统计、病毒处理结果统计、病毒发现触、方式统计、趋势图表、按分组、按终端、按病毒名称； |
| 黑白名单 | 支持手动导入、导出黑白名单，添加黑白名单。支持通过文件导入添加黑白名单； |
| 支持通过文件数字签名添加黑白名单管理； |
| 病毒扫描 | 支持信任区设置，病毒扫描或实时防护时不扫描目录或文件； |
| 病毒扫描支持扫描所有文件和仅扫描程序及文档文件设置，支持对压缩包文件设置最大扫描层数和大小，当发现压缩包内存在病毒时，还需继续扫描压缩包内其他文件； |
| 支持对终端当扫描到感染型病毒、顽固木马时，自动进入深度查模式，可设置禁止终端用户管理路径或文件白名单、禁止终端用户管理扩展名白名单、扫描时不允许终端用户暂停或停止扫描任务； |
| 支持扫描资源占用设置，可设置不限制、均衡型、低资源三种模式； |
| 支持对压缩包内的病毒扫描，支持多层压缩包的扫描，可自定义配置压缩包的扫描层数，至少大约10层模式下的扫描； |
| 主动防御 | 支持对进程防护、注册表防护、驱动防护、U盘安全防护、邮件防护、下载防护、IM防护、局域网文件防护、网页安全防护、勒索软件防护； |
| 终端病毒处理弹窗 | 客户端弹窗支持免打扰模式和智能模式，使用免打扰模式可以对不能弹窗的终端设备中避免弹窗。使用智能模式是智能调整弹窗，对已知的病毒自动处理，对未知的病毒提示处理； |
| 杀毒引擎 | 支持不少于三个杀毒引擎混合使用，提高病毒检出率； |
| 服务要求 | 两年免费质保及病毒库更新。 |

**3、端点检测和响应系统（EDR）**

|  |  |
| --- | --- |
| **技术指标** | **技术规格要求** |
| 基本要求 | 提供不少于450节点许可 |
| 全网风险可视 | 支持当前待处理高危风险展示，包括弱口令、待处理病毒、待处理漏洞数据，并支持一键跳转到对应处理页面； |
| 支持控制台动态更新显示全网终端安全状态分布，包括：终端总数、在线终端数、防护中终端数、异常设备数； |
| 支持查看当前安全防护信息数据，包括渗透追踪防护、勒索防护数据、病毒防护数据、系统登录防护数据、web请求防护数据； |
| 支持实时查看当前安全动态； |
| 一体化安全策略 | 只支持自定义安全策略、安全策略可继承，内置多个初始策略模板，包括防护模板、审计模板； |
| 支持通过对终端制定模板的方式做到一键策略下发； |
| 系统性能监控 | 支持对CPU使用率监控、内存占用率监控、磁盘读写监控、上下行流量监控； |
| ★支持对CPU、内存、磁盘读写、网络上下行流量达到配置阈值时告警，支持对CPU、内存达到一定阈值时客户端进行熔断；**（提供截图证明)** |
| 系统安全性模块 | 支持对系统登录行为进行一定的限制，可设置单个IP请求时间、登录失败次数、IP临时锁定时间； |
| 支持业务间流量东西向隔离功能，包括IP、端口、协议、流向等细粒度权限控制； |
| 支持登录防护，包括以系统账号为粒度的异常登录防护、支持4个任意维度（任意IP，任意域名，任意计算机名，任意时间）的系统登录访问策略设置； |
| 具有系统漏洞扫描和修复功能，提供真实漏洞补丁； |
| 防病毒模块 | 支持对资产进行快速扫描、全盘扫描、自定自定义扫描，并对病毒扫描结果进行导出； |
| 支持自定义病毒处理方式，包括自动处理、记录、删除。优先对病毒文件进行修复，并将修复前的病毒文件进行备份； |
| 支持从资产视角和病毒视角展示病毒查杀概况，并对病毒进行处理； |
| 支持多引擎设置，包括默认引擎、深度扫描引擎； |
| 针对Windows系统，保护文件不被恶意修改、加密等，可自定义配置保护的文件及目录，支持设置例外进程；  |
| 支持自定义病毒处理方式，包括自动处理、记录、删除。优先对病毒文件进行修复，并将修复前的病毒文件进行备份； |
| 高级威胁防护模块 | ★支持对本机的扩展行为（信息收集、权限提升）进行监测，防止提权行为和信息泄露；**（提供截图证明）** |
| ★识别渗透过程中的隧道代理（端口映射、端口转发、内网代理），可阻断隧道代理搭建行为；**（提供截图证明）** |
| 对失陷后主机远控持久化行为进行检测（反弹Shell、远程控制），可阻断远控；**（提供截图证明）** |
| ★对内网的恶意攻击行为进行识别（漏洞利用、横向移动），可阻断恶意探测行为；**（提供截图证明）** |
| 告警功能 | 告警类型包括：护网高级威胁、系统防护、网络防护、Web应用防护； |
| 告警内容至少包括：资产名称、IP地址、日志类型、风险概况、风险评级、事件发生时间等详细内容； |
| 告警方式包括：邮件告警、Syslog、短信告警及SNMP trap； |
| 云端威胁鉴定 | 联动威胁情报，支持对外联IP、DNS解析、可疑文件进行情报鉴定； |
| 集中管控 | 管理平台支持一键设置客户端卸载密码、一键卸载监控端、一键解除绑定、一键停止/恢复所有防护、一键关闭/重启主机、一键重启客户端、一键迁移资产、一键获取端上日志； |
| 支持导出已安装客户端程序的资产清单； |
| 能够通过统一的管理中心对多个服务器或主机进行监控； |
| 服务要求 | 三年免费质保。 |

**4、威胁狩猎与溯源系统**

|  |  |
| --- | --- |
| **技术指标** | **技术规格要求** |
| 硬件要求 | 2U，内存≧32G，千兆网口≧2，冗余电源； |
| 性能要求 | 沙箱数≧4；伪装代理数量≧16；沙箱种类≧32； |
| 安全要求 | 产品完全基于KVM架构，并在访问策略、进程、流量等方面采取严格的技术管控措施防止攻击逃逸，并且具备逃逸告警功能; |
| 部署要求 | 支持硬件部署，软件部署，分布式部署，客户端可集群横向扩展; |
| 沙箱仿真模块 | windows沙箱服务依托真实的虚拟服务器，有独立的含操作系统的虚拟化环境; |
| 应用服务类：支持wiki、bbs、discuz、ecshop、espcms、websphere、phpmyadmin、confluence、hadoop、crm、oa、tomcat、mailbox、jboss、zabbix、struts2、jenkins、weblogic、vpn、joomla等不少于20种高交互应用服务类沙箱； |
| 系统服务类：支持ssh、redis、mysql、ftp、samba、memcahed、sqlserver、portcheat、momgoob、telnet、mysqlcheat、postgresql、ADB等不少于13种高交互系统服务沙箱； |
| 系统类：支持windows与centos沙箱，windows沙箱支持登录和交互操作，centos沙箱支持自定义上传业务仿真页面文件； |
| 工控类：支持IPMI、MODBUS、IEC104、BACNET、S7COMM、ENIP、SNMP等不少于7种工控协议的模拟，可自定义输入和修改厂商名称、商品名称、产品名称等； |
| 自定义模板：支持用户自行拓展沙箱的类型及数量，允许上传docker镜像文件，支持自定义配置环境变量； |
| 沙箱支持增、删、停、重置、编辑沙箱内容，沙箱可关联多个IP； |
| 沙箱支持调节行为灵敏度，开启或关闭流量阻断；支持自定义邮件告警级别；支持开启关闭溯源能力，自定义位置插入溯源组件； |
| 数据仿真：支持新建沙箱后，向沙箱中注入脱敏数据，增加沙箱的真实性； |
| 探针感知模块 | 探针节点：支持在不同区域部署探针，并能将网络隔离区域的攻击流量转发至沙箱；支持感知所有攻击流量，包括且不限于tcp、udp、icmp、半连接扫描等；支持监听1-65535任意端口，且不限制端口数量；支持IPV4和IPV6的部署； |
| 探针管理支持资产管理与IP管理，支持绑定多IP。资产管理支持查看资产信息及关联的沙箱信息。IP管理支持查看不同的探针详细信息，自定义关联沙箱和配置个性化标签； |
| 诱饵感知模块 | 支持不少于四种类型的反制诱饵，用户自定义上传后缀为EXE的反制程序并关联沙箱，伪造敏感信息，诱骗攻击者进行下载； |
| 一键免杀：攻击反制木马支持自动化静态免杀、加壳、多态，保证反制功能的强力效果； |
| 办公网诱饵：支持PC诱饵发布功能，通过agent在PC上发布与沙箱相关的虚假信息，包括网页浏览记录、网站登录密码、RDP连接记录、登录域凭据等； |
| 文件诱饵：支持对已有文件word/excel/ppt加工，散布虚假信息到内网各处，感知攻击者访问行为； |
| 邮件诱饵：支持向特定邮箱发送邮件诱饵以及附件，感知邮件入侵行为； |
| 主机诱饵：通过将用户编辑的虚假信息，散布到linux主机上，迷惑攻击者； |
| 互联网诱饵：支持Github与Gitee代码伪装服务，自动化发布代码项目至GitHub与Gitee网站； |
| 智能蜜网模块 | 一键探测：支持一键感知探针节点所在网络的资产信息，分析当前网络状态； |
| 一键关联：基于探测结果和智能算法，支持蜜网一键化部署，将探针节点和无探针感知节点自动关联至对应沙箱，快速形成欺骗蜜网，简化布防操作； |
| 溯源反制模块 | 支持对黑客溯源功能，形成黑客溯源/黑客画像页面，溯源真人白名单标记，对溯源结果按照国内/国外/内网分类并展示，可提供对黑客备注功能； |
| 支持分析黑客的身份信息和设备指纹信息，包括IP地址、社交网站真人身份、设备指纹、操作系统、浏览器等，支持不少于10种社交ID溯源能力； |
| 黑客画像支持展示攻击者身份、备注、源IP、内网/公网IP、浏览器信息，黑客轨迹聚合该黑客所有攻击事件，支持攻击源探测，探测攻击源的服务与端口；  |
| 可基于现有的设备指纹进行设备指纹碰撞，反查攻击者的历史溯源信息，补充溯源信息； |
| 具备攻击反制功能，可以反向控制攻击者设备，获取对方设备信息，进行交互式反制操作，支持交互shell、文件上传下载、电脑截屏、摄像头拍照等操作，支持获取qq、wechat、手机号、CS、iphone设备信息、xshell、navicat、Git、Email、域名及对应的用户名等应用的用户ID和关键信息，便于身份溯源； |
| 获取精确设备指纹：可获取设备的操作系统、设备类型、主板信息、硬盘序列号、CPU类型、BIOS信息、GPU类型、显示器名称、IDE名称、声卡名称、内存条制造商及名称、硬盘名称、主机品牌、物理机接口、当前用户等信息； |
| 行为记录模块 | 对于Windows沙箱的远程RDP攻击，支持录制攻击过程的视频，可回放攻击过程；对于SSH沙箱的攻击，支持以视频的形式回放用户的命令行操作记录； |
| 支持记录攻击者所有攻击行为，通过时间线展示，并可从攻击源、攻击手法、攻击资产、隔离沙箱、攻击类型、时间线等维度进行筛选查看； |
| 支持基于ATTCK的攻击事件回放，并以时间轴的方式展示重点攻击手法及事件，支持从攻击时间、攻击资产、攻击手法、来源IP、事件类型等进行筛选； |
| 支持记录各类Web应用与系统服务登录爆破，支持识别记录Web攻击类型，支持识别僵木蠕攻击、漏洞利用手法； |
| 支持将不同攻击者对不同沙箱的攻击单独归并，分别展示为事件，可通过攻击事件回溯查看该事件所有攻击行为； |
| 支持记录攻击者上传的任意文件，并分析其文件类型、MD5等判断其是否为恶意木马； |
| 支持威胁情报数据通过在线或离线包的方式同步至本地化威胁情报中心； |
| 支持记录攻击者所有行为，并能识别真人与扫描工具，至少能识别7种扫描工具； |
| 可视化模块 | 支持大盘展示受攻击资产、探测与入侵事件统计、受攻击沙箱等； |
| 支持蜜网拓扑图，展示管理端与沙箱、探针节点等之间的拓扑关系，以及欺骗资产在当前网络的覆盖情况； |
| 针对安全攻击事件支持多维度归并分析，包括但不限于攻击事件、攻击者、攻击时间维度等； |
| 查看事件页面，能基于攻击者、攻击资产、隔离沙箱、风险等级、攻击起始时间等进行筛选，并能通过攻击源和过滤IP进行搜索； |
| 支持生成html、doc、pdf、excel等格式的分析报告； |
| 管理要求 | 账号权限分离，提供超级管理员、管理员、普通用户、审计员角色权限； |
| 支持Radius认证登录； |
| 支持将post攻击数据推送到指定的http服务器； |
| 支持威胁事件的实时告警、并提供事件处理功能； |
| 支持白名单配置，包含扫描白名单，系统访问白名单配置等操作； |
| 支持扩展功能开关，包含post内容捕获、攻击源探测、逃逸检测、攻击反制、pcap包下载等操作； |
| 服务要求 | 三年免费质保。 |

**5、代码审计系统**

|  |  |
| --- | --- |
| **技术指标** | **技术规格要求** |
| 硬件规格 | 配置不少于2颗CPU，内存≧128G，存储≧4TB，≧2个千兆电口； |
| 源代码缺陷分析功能 | 支持C/C++、Objective-C、C#、Java、PHP、Swift、Go、Python、Cobol、Node.js、Kotlin、SQL等主流编程语言开发的软件源代码的缺陷检测； |
| 支持代码注入、跨站脚本、输入验证、危险函数、代码质量、API误用、密码管理、异常处理等常见安全缺陷问题的检测，二级缺陷类型不低于1600个； |
| 支持用户对源代码缺陷分析模板的灵活配置，具体到每一个缺陷类型； |
| 支持函数白名单功能，检测过程中自动识别白名单函数进行路径裁剪，减少误报； |
| 支持文件/文件夹白名单功能，可以对多个文件或文件夹进行过滤，不统计该文件和文件夹下检测的问题结果，提高系统检测精准性； |
| 支持根据检测语言类型配置可信数据源，提高检测准确性。可信数据源包括命令行参数、web表单、json字符串等，界面可选可信源配置类型应不少于15种； |
| 支持对检测失败的任务重新发起检测，无需重新上传代码；  |
| 支持通过产品界面下载单个检测任务的检测日志； |
| 检测完成后，系统能够自动以邮件方式将检测结果通知到指定人员； |
| 支持配置单个检测任务的回调地址，检测任务结束后，可以主动通知第三方系统检测任务状态和任务摘要信息； |
| 源代码缺陷审计功能 | 能够对源代码安全扫描结果进行汇总，并按照问题的严重性和可能性进行威胁级别的划分，如高、中、低等多个级别； |
| 能够针对同种类型的安全问题成因路径进行统一展示，便于找到最佳修复节点； |
| 能够迅速定位某一特定源代码安全问题所在源代码行，对问题产生的整个过程进行跟踪； |
| 能够提供中文的源代码安全问题分类、问题描述及修复建议； |
| 能够对当前问题进行审计，修改问题等级以及修改问题状态为是问题、不是问题、遗留问题； |
| 能够记录结果的审计信息，包括人员、时间和审计信息等。 |
| 能够对检测结果按照缺陷类型、审计状态、文件名进行过滤查询； |
| 支持按照安全缺陷、质量问题、错误编码分类对缺陷进行分类显示，能够对检测结果列表进行全文检索； |
| 支持审计信息携带，能够将上一版本的人工审计信息携带到下一版本的检测结果中，无需重复审计，降低审计成本； |
| 能够根据任务名称、创建者、开发语言、检测状态、检测开始时间、问题数量等多种条件对源代码检测任务进行查询，针对每一个源代码检测任务能够展现相关信息，如任务名称、开发语言、检测开始时间、检测完成时间、检测状态、问题总数、等级分布以及创建者； |
| 统计分析功能 | 能够根据检测时间、检测方式、任务类型、缺陷等级选择一至多个检测任务进行统计，统计显示各部门任务数、总代码行数、缺陷总数、平均缺陷密度等信息； |
| 支持部门维度的数据统计，展示部门的缺陷数量、平均缺陷密度统计信息； |
| 支持缺陷类型维度的数据统计，能够展示出现次数最多的TOP10缺陷类型及数量； |
| 支持配置缺陷类型集合作为统计分析模板，可以统计指定缺陷类型的检测结果； |
| 源代码缺陷分析报告功能 | 检测报告应能够根据用户角色分为概要报告和详细报告：概要报告主要包括问题等级及问题类型等基本统计信息；详细报告除了包括问题等级及问题类型等基本统计信息外，还应包括问题分类、问题描述、修复建议、风险点、问题跟踪信息、审计日志等详细信息； |
| 报告内容可对问题等级、问题类型、修复建议、跟踪路径、审计日志根据需求进行定制； |
| 系统管理功能 | 系统为B/S架构，支持多用户同时使用浏览器访问，支持4个检测任务并发执行，检测任务并发数可通过产品界面配置； |
| 支持自定义角色权限； |
| 支持检测任务队列管理，可以通过界面对排队中的任务实行队列置顶、暂停操作，可以删除正在执行的任务； |
| 能够提供系统操作日志，记录用户的关键操作；能够提供系统错误日志，记录关键的错误信息；  |
| 可支持通过系统界面下载系统日志和引擎日志；  |
| 能够实时查看系统运行状态，包括CPU、内存、硬盘、数据库等信息，引擎内存可通过产品界面配置； |
| 支持配置统计分析模板，统计分析模板可设置访问权限，可以统计指定缺陷类型的检测结果；  |
| 提供自定义检测规则功能，自主添加检测规则用于源代码缺陷检测； |
| 提供缺陷知识库在线查看，能够根据缺陷类型、关键词、威胁等级等条件进行搜索，分语言和类型显示该缺陷的等级、详细信息、修复建议和参考信息内容； |
| 提供缺陷知识库维护功能，可上传文件导入检测规则知识库，实现知识库的在线更新。可对任意一条缺陷的威胁等级、详细信息、修复建议进行修改和重置，同时可以一键重置全部已修改的知识库；  |
| 提供系统级数据统计功能，可查看系统使用状况，可展示系统使用的部门数、用户数、激活用户数、月活跃用户数，源代码数；  |
| 提供系统级审计日志报告导出功能，可导出和下载指定时间段内的审计日志报告；  |
| 第三方工具集成能力 | 系统支持本地直接发起检测任务，也可以从SVN、GIT、Azure DevOps 、StarTeam、ClearCase 等代码仓库获取代码发起检测任务，同时源代码来源支持FTP和共享目录；  |
| 支持构建工具集成，如Maven，Gradle，支持自动获取被测源代码的第三方依赖进行检测； |
| 可以从Visual Studio、Eclipse、intelliJ直接发起检测任务并查看检测结果，对结果进行审计； |
| 对外提供二次开发接口，支持外部系统添加用户、发起检测任务、获取任务结果和缺陷详情以及离线报告生成、查询、下载等功能；  |
| 服务要求 | 三年免费质保。 |

**6、数据加密系统**

|  |  |
| --- | --- |
| **技术指标** | **技术规格要求** |
| 产品规格 | 2U机架式，双交流电源，2GE板载管理口，4GE板载接口，1×接口板卡插槽；≧16GB内存，≧2TB硬盘，配置10个数据库(IP+Port)授权； |
| 部署方式 | 支持旁路部署方式，实施时不需要改变业务系统及数据库系统的网络拓扑结构，实施后不会影响业务系统对数据库系统的访问； |
|  数据库类型及平台 | 支持Oracle、SQL Server、MySQL（包括Percona和Mariadb）、达梦、人大金仓、瀚高、神通、GBase 8s、GaussDB A等数据库；支持hdfs、Linux操作系统等文件系统加密；支持Linux、Windows、AIX、中标麒麟、银河麒麟操作系统；支持x86、ARM等平台； |
| 存储加密能力 | 支持以表空间为单位进行数据加密，加密的表空间的数据在数据库中以密文格式存储； |
| 不限制加密数据的数据类型，支持数据库系统所有的内置数据类型； |
| 提供图形化的数据加密配置； |
| 密钥管理 | 多级密钥体系，至少有根密钥和数据加密密钥两级，使用根密钥对数据加密密钥加密，以保证密钥的安全性； |
| 加密系统须保证提供数量足够的密钥，对不同的加密对象使用不同的密钥进行加密，以保证加密数据的安全性； |
| 加密系统须提供密钥备份与恢复功能，备份的密钥可以由加密系统导出到安全介质进行存储，备份出的密钥可以恢复到新部署的加密系统且恢复后的加密系统可以正确地进行加密与解密操作； |
| 独立权控 | 被保护数据表的权限控制应独立于数据库的权限控制，防止数据库用户的权限提升引起的数据泄密； |
| 具备基于密文的增强访问控制，防止DBA及高权限的数据库用户对敏感数据进行越权访问； |
| 授权用户对受保护数据的访问能够限定到指定的IP，只有在指定的IP上才可以访问受保护数据，实现更加精确的授权和访问控制； |
| 能够屏蔽在数据库服务器本地登录到数据库系统访问保护表的非法访问行为； |
| 加密算法要求 | 支持AES128、AES256国际标准加密算法，支持国密SM4算法； |
| 透明性 | 支持SQL、PL/SQL、JDBC、ODBC的透明性，应用系统、数据库内存储过程和自定义函数不需要改造； |
| 支持Oracle的RAC、异常数据恢复、MVCC、分区等高端特性，数据库内定义的主外键约束不受影响，Check、Null等完整性约束不受影响； |
| 加密后，对数据同步透明，原有的数据库实例间数据同步规则和过程不受影响； |
| 支持数据库现有的管理工具和维护工具的透明性，数据库管理员依然可以使用现有工具实现数据库管理、备份恢复和数据库运行状态维护； |
| 容灾能力 | 支持主、从互备，及异地灾备等多级容灾能力，防止主机故障、网络故障、程序故障引起的业务损失。同时各种容灾手段应能快速启用、自动切换，且切换期间能保证数据一致性，业务不受损失； |
| 主、从服务之间的切换应能在3秒之内完成；  |
| 提供离线解密工具，当数据库不能正常启动时，通过离线工具对密文数据文件执行解密操作，还原数据，防止数据丢失； |
| 产品具备应急机制，可以根据用户需要启用，能够在紧急情况下保证加密数据的安全性和业务的连续性； |
| 状态监控 | 提供安全服务运行状态监控与诊断机制，可监控安全服务的运行状况，并对异常情况进行处理，保证安全服务健康运行； |
| 系统管理 | 支持三权分立，系统默认设定系统管理员、安全管理员、审计管理员三种角色，可以新建用户，可以为新建用户分配权限； |
| 具有自身安全审计功能，可以对加密系统的所有用户操作进行审计记录； |
| 具有硬件网卡管理功能，可以实现管理口与业务口分离，且支持多个业务口同时工作； |
| 服务要求 | 三年免费质保。 |

**7、数据库权限管控系统**

|  |  |
| --- | --- |
| **技术指标** | **技术规格要求** |
| 配置 | 本次配置16个数据库实例； |
| 硬件规格 | 2U机架式，双电源，≧6个千兆电口，≧16G内存，≧128G SSD，≧2T存储空间； |
| 数据库支持 | 支持ORACLE、SQL SERVER、DB2、MySQL、PostgreSQL、ODPS、informix、达梦、impala、mongdb等主流数据库、国产化数据库、大数据平台、云数据库； |
| 数据智能发现 | 具备敏感数据探测能力，自动发现SCHEMA、表中的敏感资产，系统内置的敏感数据类型至少包括：个人敏感信息：包括中文姓名、身份证、银行卡、医师资格证书、医师执业证书、护照、军官证、中国护照、港澳通行证、永久居住证、大陆居民往来台湾通行证、韩文姓名、英文姓名、姓名拼音等个人信息；机构敏感信息：组织机构代码、组织机构名称、医疗机构登记号、营业执照、社会统一信用代码、税务登记证、开户许可证、证券名称、证券代码、基金名称、基金代码、英文公司名等与企业机构相关的信息；其它基础信息：电话、电子邮箱、地址、邮政编码、IP地址、日期、货币金额、json串、车牌号码等；以上功能投标时需提供截图证明 |
| 支持敏感发现结果列表展示，包括表名、列名、敏感类型、数据抽样示例等，支持对发现结果进行校正； |
| 支持从表格、表格列、SCHEMA等维度归类敏感数据资产，形成敏感资产集合进行独立管理；  |
| 身份准入 | 支持身份的多因素认证，至少应支持应用程序名、IP地址、主机名、操作系统账户、数据库用户、数字证书、身份敏感标签、日期、时间、时间域、身份类别、有效时间、应用用户名、终端IP等因素的任意组合，系统根据多维身份管理策略，自动判别登录主体的合法性，如不符合设定的身份管理策略，登录失败； |
| 支持识别真实应用及SQL管理工具的MD5值，防止假冒应用及假冒SQL管理工具违规访问数据库；**（提供功能截图证明）** |
| 支持为敏感数据管理人员身份分发唯一的数字证书，每张数字证书只能载入一个唯一的U盾，以实现在数据库用户密码被泄露的情形下，仍能阻止非法用户登录目标数据库，解决仅依靠密码认证带来的安全不足问题；**（提供功能截图证明）** |
| 支持通过不删除账户的方式，在系统中回收资产授权权限； |
| 身份治理 | 对登录访问事件信息中的主体信息与身份信息进行比对，对未命中的主体身份，快速发现进行治理； |
| 直连数据库 | ★在反向代理模式下，通过在数据库服务器上安装安全代理插件，实现对于通过SQL管理工具或本地等直连数据库的违规连接行为进行准入控制，防止非法人员绕过安全系统，违规对数据库进行访问；**（提供功能截图证明）** |
| 安全登录 | ★支持数据库运维工具免密登录功能，当数据库管理人员通过Toad或SQL DEVELOPER等工具登录运维数据库时，通过数据库账号与数字证书的绑定，数据库管理员在运维PC工具中无需输入数据库用户名密码即可登录已授权访问的数据库，避免运维数据库用户和密码泄漏，保障账号安全；**（提供功能截图证明）** |
| 通过账号托管功能，运维人员使用分配运维账号，运维用户与数据库用户及密码进行映射绑定，运维人员在不知道数据库真实密码的情况下，即可完成对数据库的运维和管理，全面保障数据库安全；**（提供功能截图证明）** |
| 访问控制 | 针对敏感数据集合的访问，任何账户（包括DBA\SYSDBA\Schema User\any权限等用户）都需要通过授权才可以访问，对不具备访问权限的操作，明确阻断拒绝，并提示“安全权限不足错误”， 实现用户权限分离管理； |
| 支持拦截指定对象的ALTER TABLE、ALTER TABLESPACE、DROP DATABASE、DROP TABLE、DROP TABLESPACE、DROP USER、TRUNCATE等高危操作行为，支持数据库权限变更行为管控； |
| 支持修改、删除等操作的行数控制，避免数据大量泄漏。 |
| 敏感数据脱敏 | 支持基于列的业务类型，设置脱敏策略，实现相同的业务类型脱敏； |
| 支持运维动态脱敏，实现脱敏的三层关联，针对不同用户返回对应的预授权结果，脱敏规则需要支持以下脱敏算法： 1、放行：对于已授权用户，返回真实数据；2、返回空：对含有敏感表格或敏感列的数据结果返回为空值；3、遮盖：全遮盖：默认以遮盖符‘\*’替换敏感列的值；4、部分遮盖：对敏感列的值进行分段，替换其中的一段或数段值；5、随机映射：对数值、字符或字符串进行随机映射处理；以上功能投标时需提供截图证明 |
| 工单管理 | 采用基于WEB界面的工单管理模式，而非授权码方式，通过工作流的方式对敏感表格和敏感SQL访问授权，形成逐级审批机制，只有当访问申请被工作流中的所有审核者审批通过时，才可在合理权限内访问数据库中的敏感资产，无需访问者进行二次输入，避免授权码泄漏带来的非法访问；**（提供功能截图证明）** |
| 支持以图形化形式直观展现工单审批流程； |
| 工单申请支持按不同的库，走不同的审批人方式； |
| 审计 | 支持SQL命令（包括查询、新增、修改、删除等行为）的细粒度审计和分析，并详细记录管理用户的行为信息，包括事件ID、连接ID、规则名称、数据库主机、目标数据库名称、数据库实例名、客户端IP/端口、主机名、数据库用户名、物理地址、交换机端口、应用名称、应用用户、企业用户、命令类型、资产名称、执行时间、影响表数、错误号、审计级别、响应行为、风险级别等； |
| 数据库监控 | 支持统计数据库请求数、会话数、流量信息； |
| 报表管理 | 支持日报、月报、周报等生成，导出格式支持PDF/word； |
| 系统登录 | 支持与AD、LDAP系统联动登录系统； |
| 平台安全 | 平台具有安全审计员、安全保密员、系统管理员三种角色，实现三权分立； |
| 支持对平台用户的密码复杂度（数据、大小写字母、特殊字符、密码长度等）、有效期、复杂度、密码错误锁定策略等进行限制，有效期过后提供登录重置密码或禁止登录需联系管理员处理2种处理方式，以确保平台自身账户的安全； |
| 告警 | 支持以图形、列表等方式查看告警信息，以列表形式展现的告警信息应当包含告警时间、告警内容、告警等级、用户IP、数据库代理IP、事件等； |
| 告警方式至少包括：邮件、页面、短信； |
| 安全告警支持基于任意组合订阅的模式，实现个性化告警订阅管理； |
| 日志外发 | 支持通过kafka的方式进行日志外发，支持审计、告警等日志外发； |
| 国产化兼容 | 与达梦数据库兼容（提供兼容性证书）；与巨杉数据库兼容（提供兼容性证书）；与南大通用数据库兼容（提供兼容性证书）；与神舟数据库兼容（提供兼容性证书）；要求至少满足其中任意三项兼容性证明，**投标时需提供以上相关证书复印件并加盖公章；** |
| 服务要求 | 三年免费质保。 |

**8、数据库脱敏系统**

|  |  |
| --- | --- |
| **技术指标** | **技术规格要求** |
| 敏感数据发现 | 支持数据源管理功能，主流数据源类型包括但不限于MySQL、Oracle、Db2、MSSQL、PostgreSQL、Greenplum、SybaseASE、Informix、Hive、ODPS、MariaDB、Clickhouse、Elasticsearch、MongoDB、MariaDB、达梦、GBase8A、Kingbase，同时支持新增本地文件【xls、xlsx、csv、txt】、SFTP\FTP数据源的添加； |
| 支持自动数据识别发现敏感项，包括敏感表和敏感列以及敏感项的动态变化； |
| 提供数据目录，可以查看数据的分布情况，包含表级别分布和列级别分布；同时提供包括数据库梳理、敏感表数量、识别字段数、敏感列数和已经梳理占比情况等信息； |
| 支持数据分级分类任务任务的管理功能，包括但不限于务名称、数据源名称、主机、发现结果、状态、次数、周期、创建时间、最新发现时间、操作。提供查看任务详情，可以查看以图表形式展示当前数据源分类分级的概况； |
| 敏感数据脱敏 | 支持主流字符集如gbk、gb2312、gb18030、utf8、utf8mb4等； |
| 支持自定义脱敏算法模板库，用户可将若干脱算法略组合成为适用于该场景的脱敏算法模板库，脱敏模板库定后，可被重复利用； |
| 支持脱敏任务的配置功能，提供数据库到数据库、数据库到文件、文件到数据库、文件到文件流程的脱敏任务新增功能，支持数据处理配置和脱敏算法的配置； |
| 支持脱敏任务的展示功能，包括但不限于任务名称、脱敏流程、任务状态、执行次数、执行周期、新增时间、最近执行时间、执行耗时和操作等信息，同时支持任务的编辑、查询功能； |
| 开启脱敏任务审批后，用户提交脱敏任务审批后，权限管理员可以进入该界面进行脱敏任务的审批，审批通过后方可执行脱敏任务； |
| 可制定要脱敏的表，自由选择全量或增量抽取数据，可基于字段自由配置增量条件； |
| 支持自动同步源数据表主键、索引、唯一约束至目的表； |
| 支持覆盖原表脱敏； |
| 脱敏报表 | 支持指定时间段内的脱敏任务统计报表，包括并不限于脱敏任务名称、脱敏执行时间、数据库类型、任务概况、脱敏算法分布情况、脱敏数据量占比情况，同时可配置对比时间周期，从而获取脱敏的变化情况； |
| 脱敏算法 | 静态脱敏支持不低于20类，240种及以上的脱敏算法； |
| 对类别属性的数据进行编码，去除字段内容含义，仅保留类别区分性。适用于机器学习等数据分析中需保留标签区分性的场景； |
| 编码，根据所选参数指定的编码方式对数据进行编码。支持的编码方式有：UTF-8/GBK； |
| 对数值类型的数据进行标准化缩放，使得数据均值归为0，方差归为1。本算法脱敏后的数据基本保留数据分布类型，可后续用于常见的分类、聚类等数据分析任务； |
| 系统管理系统管理 | 支持用户管理功能，用户可以进入该界面新增自定义用户，并关联自定义角色。同时支持用户权限的管理功能，新增自定义用户后，权限管理员需要进行授权后，自定义用户方可登录，提供自定义角色的管理功能，每个角色可以关联不同的功能权限； |
| 提供管理用户登录相关的安全配置； |
| 支持配置外部日志的存储以及脱敏任务是否需要审批的开关； |
| 提供所有用户的相关操作日志的展示； |
| 服务要求 | 三年免费质保。 |

**9、数据水印系统**

|  |  |
| --- | --- |
| **技术指标** | **技术规格要求** |
| 系统易用性 | 系统基于B/S架构，采用HTTPS方式远程WEB安全管理，提供中文操作界面,无需安装管理客户端或者代理即可使用； |
| 数据库支持 | 支持Oracle、SQLServer、Mysql、PostgreSQL、ODPS等主流数据库为源数据库和目标数据库； |
| 文件支持 | 支持excel、csv、txt文件为源文件和目标文件，支持FTP和本地文件； |
| 水印数据管理 | 内置常见的数据特征库用于自动发现，包括身份证、手机号、固定电话、银行卡、台湾居民来往大陆通行证、港澳通行证、护照号等； |
| 内置常见数据类型特定的水印算法，可根据数据类型发现结果自动匹配水印算法； |
| 水印方式 | 支持数据库到数据库，数据库到文件，文件到数据库，文件到文件的水印分发方式，满足各类水印分发需求场景； |
| 水印过程数据不落地，减少中间过程数据泄漏风险； |
| 水印算法 | 支持伪行、伪列、无痕三种水印算法； |
| 支持手动干预调整数据水印算法，满足用户多样化的数据水印需求； |
| 水印具备鲁棒性，水印算法具备密钥管理无法被篡改，数据部分遭到破坏后仍能进行有效溯源； |
| 水印任务 | 支持任务调度执行，可立即执行，或者自定义任意启动时间，支持周期执行（按天/周/月）； |
| 支持查看作业的执行结果，包括所用时长、起始时间、创建人等相关信息； |
| 支持水印任务报告，可在任务界面直接查看水印失败日志等详细信息，提高业务效率； |
| 支持水印任务启用/停止、水印任务结果下载等操作； |
| 系统支持水印信息管理，提高水印信息的可复用性； |
| 数据库溯源 | 支持Oracle、SQL server、MySQL、PostgreSQL、ODPS等数据库水印溯源，溯源结果展示包括水印具体信息，数据源信息等，可快速定位泄漏源； |
| 文件溯源 | 支持FTP、本地文件水印溯源，支持txt、csv、excel格式，溯源结果展示包括水印具体信息，数据源信息等，可快速定位泄漏源； |
| 三权分立 | 提供系统管理员、安全管理员和审计管理员来管理水印设备，权责分离； |
| 安全审计 | 系统针对水印产品操作人员的操作行为进行审计记录，可以由审计管理员进行查询，具有自身安全审计功能； |
| 状态监控 | CPU、内存、磁盘使用状态动态展示。内核、CPU、磁盘、网卡、磁盘IO实时诊断； |
| 权限管理 | 具备完善、统一的权限管理体系，可以针对不同用户、不同角色、不同业务系统实现数据行级的权限控制，完成用户建立、用户分配、用户身份验证等管理功能，满足系统用户所有资源信息具备最小颗粒度的可配置、可分配的能力，保证针对具体的使用用户进行分配，每个用户仅能使用其分配的资源； |
| 公共服务接口 | 支持SYSLOG/SSH等接口设置； |
| 服务要求 | 三年免费质保。 |

**10、数据安全管控分析服务**

|  |  |
| --- | --- |
| **技术指标** | **技术规格要求** |
| 业务建模 | 业务场景建模能力：面向多部门协同的业务场景或复杂的数据流转场景，根据数据的流向，利用数据流节点，采用简单的元件拖拽、连线的操作方式对其数据流转进行可视化的拓扑配置和统一管理，基于业务需求对其节点及节点之间的数据流转设置监控策略。基于业务的数据流转拓扑作为数据、业务和人员安全监控的参考基线，包括节点对象的访问量、访问流量、访问速率、请求延时、异常访问和敏感数据访问的监控，同时支持对特定数据的全网数据流转拓扑自动梳理；**（需提供原型演示）** |
| 基于拓扑建模基础，生成业务大屏，对业务相关风险进行可视化展现，包括SQL注入、漏洞攻击、账号安全、数据泄露、违规操作、可疑通信等；**（提供界面截图）** |
| 规则管理 | ★不少于20种数据安全预设场景模型，不依赖规则库包括数据泄露、敏感数据大量返回、敏感数据遍历、账户安全、接口异常、越权请求等各类数据安全事件；**（提供界面截图）** |
| 可以自由清晰定制场景规则，点选函数便可配置相关规则，避免规则语言手动写入的繁杂设置，通过简单的规则配置，通过匹配、抽取、统计、判断引擎从海量数据中设置数据安全事件规则；**（提供界面截图）** |
| 敏感数据安全监管 | 敏感数据访问监控：支持基于异常操作分析模型，及时发现敏感数据的高危操作行为并告警，包括敏感数据的大量返回、敏感数据的异常访问、敏感数据遍历、敏感数据泄漏等；**（提供界面截图）** |
| 敏感数据流转监控：支持对归集、共享、交换的数据流转的流量分析，捕获数据的访问和流转，记录整个流转过程及数量，以关联形式存储和展现，形成整个数据流转链路，同时实时发现异常数据流转路径，并及时告警；**（提供界面截图）** |
| 支持对敏感库、敏感表、敏感字段的数量、分布关系、访问热度登进行罗列排序展示，同时对数据资源的元数据管理标签进行展示，统计各敏感等级的数据资产，关联各敏感数据资源的告警事件，实现对敏感数据数量、分布、关系、告警事件等多方位的安全监管；**（提供界面截图）** |
| 敏感接口安全监管 | ★数据接口安全监控：支持数据接口调用审计，建立数据接口安全基线，包括数据接口的调用频率、目的IP、时间等维度，对偏离安全基线的数据接口调用情况及时告警；支持长时间未调用的僵尸接口的发现和告警；支持数据接口健康状况的实时监测，及时发现数据接口的访问高延时、返回报错、404异常访问等安全报错并及时告警，以保障业务的连续性；**（提供界面截图）** |
| 资产识别梳理能力**（需提供原型演示）** | 对安全资产的全面分析展示，支持采用自动发现、手工录入等方式对全网基础网络资产信息进行统一梳理和统计，通过对资产从部门、系统等多方位的类型划分，以图表形式帮助客户整体掌握当前组织结构下，资产总量、各单位的系统数量、系统所使用的资产数量等信息 |
| 规则引擎分析能力**（需提供原型演示）** | 支持用户根据自身业务特性，通过【规则匹配】、【规则抽取】、【规则统计】、【规则判断】四大引擎编排内容，对来源、目标、标签等因子的自由定义组合成规则，再针对不同场景匹配不同规则组合形成对请求端信息、访问请求、行为特征，目标端所返回的数据量、数据敏感度等进行管控的针对性策略，灵活自定义数据安全场景规则，变动告警阈值和告警生效节点 |
| 智能检索 | 支持对安全告警数据进行分类检索，从检索结果可关联资产信息并一键跳转； |
| 支持不少于1000条检索结果导出，支持CSV格式； |
| ★支持智能检索语句分析，支持检索语句的中英文、拼音智能联想，支持逻辑运算符与字段值的自动提示补全；检索语句支持快速保存，历史检索语句快速导入；**（提供界面截图）** |
| 场景大屏 | 对管控平台所覆盖到的监管范围内所有数据资产的安全态势进行整体感知，通过一张屏进行多维度数据安全态势展示； |
| 支持罗列部门、主机、系统、接口、数据库、账号的资产数量；支持展示今日、本周、本月的告警总数、分类数量及告警趋势状况；支持展示数据来源及数据去向的数据接口流动情况；支持展示数据访问及接口访问的TOP排行及访问趋势；支持展示数据安全事件的工单数量及处理状态；**（提供界面截图）** |
| 共享与回流防护 | ★数据调用管控：提供应用系统接入平台调用API接口和数据的身份认证和权限控制；**（提供界面截图）** |
| 支持批量数据共享、回流、导出监管，描绘数据回流路径，实现数据共享回流监管，发现违规回流项目空间、违规回流表、违规回流云账号等信息，对异常回流进行告警；**（需提供原型演示）** |
| 安全检查平台运营 | 平台内置安全合规检查模板，支持自定义检查模板及快速下发，被检查单位按要求将检查项的证据材料上传，实现一站式的快速检查；**（提供界面截图）** |
| 数据对接 | 与杭州市数据管控平台进行对接，完成与市级平台的数据分类分级结果上报，风险共享，工单流转等内容，提供平台对接相关证明材料；（所有数据对接费用均由供应商提供，**需提供原型演示**） |
| 服务要求 | 一年 |

**11、全链路安全监管升级服务**

|  |  |
| --- | --- |
| **技术指标** | **技术规格要求** |
| 基本要求 | ★在现有数据管控平台基础上，增加云、网络及边界、应用、终端方面的安全监测能力，含资产管理升级服务、告警管理升级服务、通报处置升级服务、监督检查升级服务、知识库管理升级服务、考核评估升级服务、态势感知升级服务、事件案例升级服务，能与数据管控平台进行对接，**提供服务升级和数据对接相关证明材料；** |
| 资产管理升级服务 | 资产概况 | 支持资产总量及资产分类数量统计，支持待明确资产统计以及下级单位上报资产数量统计； |
| 支持未知资产发现趋势统计，包括流量发现、下级单位上报； |
| 支持按照单位、区域进行资产分布统计； |
| 资产发现 | 支持未知资产导出； |
| 支持未知资产二次运营后形成本地资产库； |
| 资产管理 | 支持对单位信息按地区、统计和筛选； |
| 支持按列表的方式统计展示单位信息，展示信息包括单位名称、单位简称、地区、网络数量、业务系统数量、IP数量、监管单位、主管单位、标签； |
| 能够对单位资源按单位名称、单位简称、标签字段进行查询； |
| 能够对单位资源进行添加、批量删除、导入、导出； |
| 支持按软件资产、硬件资产、IP资产分类展示资产信息，支持资产数据的批量导入、导出； |
| 支持资产自定分类； |
| 一键搜索 | 支持输入关键字对资产数据进行一键搜索，一次最多支持查询10个词组； |
| 支持显示历史检索条件； |
| 支持检索结果以资产实体的形式呈现； |
| 告警管理升级服务 | 数据归一处理 | 能够接受数据接入的数据过滤计算任务，进行数据的过滤、归并； |
| 分布式计算 | 能够提供分布式计算资源，支持流式计算任务、批量计算任务，为数据分析提供支撑； |
| 分布式存储 | 能够提供分布式存储方式，能够快速建立数据索引，并能支持快速检索； |
| 日志检索 | 支持查询检索范围选择日志类型，类型包括：告警原始库、告警资源库、流量原始库、HIVE查询库、审计日志库； |
| 选择索引后，点击搜索语句框会下拉展示通用字段、流量通用字段，以及该索引特有字段； |
| 支持搜索条件提示字段编辑； |
| 支持多值搜索，可连续选择多字段； |
| 支持日志列表中字段的过滤或排除； |
| 支持lucene语句搜索，定义语句进行英文搜索语句检索数据； |
| 日志展示 | 支持在字段区域可操作字段在“已选字段”、“可选字段”间变更、展开查看字段信息； |
| 支持字段二次搜索，在原搜索基础上可以根据字段值二次搜索； |
| 支持日志内容以“键/值”、“JSON”格式展示； |
| 通报对接 | 要求通报与浙政钉进行对接，通过浙政钉通知到具体责任人进行签收反馈整改处置； |
| 通报处置升级服务 | 支持通报流程统计，可根据多维度查询展示通报信息； |
| 通报详情支持显示多类通报相关信息，包括但不限于通报标题、通报标签、所属单位、发起单位、通报完整流程及当前所处流程、通报正文、举证信息、处理记录等；**（提供功能截图证明材料）** |
| 支持通过通报下发单位及业务系统的信息补全任务，通报接收单位补全信息返回后支持将已补全的信息直接入库； |
| 支持通报举证信息一键查询，通报处置人员可以直接定位到通报关联的原始信息进行查看； |
| 支持通过事件成果、风险成果携带相关信息辅助生成通报，支持自定义编辑通报信息内容； |
| 支持通报流程可配置，各流程的对应的处置单位可自动生成，并支持自定义调整；**（提供功能截图证明材料）** |
| 通报支持进行超时设置，针对截止时间一天内的通报进行截止时间醒目提醒；针对已超时的通报进行超时显示，并显示具体超时时间；**（提供功能截图证明材料）** |
| 监督检查升级服务 | 现场检查 | 现场检查任务至少包含待下发、任务签收、结果填报、结果签收、单位整改、整改审核和办结等状态； |
| 现场检查中提供下发任务、签收任务、填报结果、整改上报、整改审核等操作功能； |
| 支持在同一个现场检查任务下发时选择单位、系统等多个现场检查对象，同时支持针对每一个对象配置相关检查表单；**（提供功能截图证明材料）** |
| 支持在现场检查任务结果填写完毕提交时自动统计本次任务发现的各等级漏洞数量； |
| 网络安全检查任务 | 单位自查至少包含待下发、任务签收、结果填报、结果审核和办结状态； |
| 单位资产中提供下发任务、签收任务、填报结果、结果审核等操作功能以推进单位自查任务状态变化直至办结； |
| 支持在同一个单位自查任务下发时选择单位、系统等多个自查对象，同时支持对每一个对象配置相关检查表单；**（提供功能截图证明材料）** |
| 支持单位自查相关的检查通知书、自查报告等文书通过流程各环节上传到相应的单位自查任务中进行留档； |
| 支持特殊情况下对现场检查的单条或多条任务进行一键直接办结； |
| 知识库管理升级服务 | 安全知识库汇总 | 支持建立一个安全知识库，管理维护安全相关的标准、指导性文件，包括但不限于国家、省、市制定的各类标准制度规范、平台对接接口规范、标准解读等，支持上传、下载和在线阅读； |
| 考核评估升级服务 | 考核统计分析 | 支持统计每个考核任务的考核概况统计，包括考核单位数、考核任务权重、考核指标数量、最高评分、最多评分、评分top5、单项指标最低评分top5； |
| 支持按照单位过滤筛选考核任务统计页面； |
| 考核任务管理 | 支持通过任务时间、创建单位、任务状态、标签、关键字（任务名称、联络人）查询考评任务； |
| 支持对考评任务排名，支持柱状图展示考评任务单位排名、饼状图展示各分数等级分布；支持展示单位排名总分列表，包括单位名称、所属区域、单位类型、单位联系人、联系方式、单位直属性质、得分等；**（提供功能截图证明材料）** |
| 考核评分管理 | 支持对考核评分任务评分； |
| 支持展示考核评分任务的任务名称、任务状态、任务时间、单位填报时间、创建单位、任务联络人及其联系方式、考评进度； |
| 支持通过任务时间、创建单位、任务状态、标签、关键字（任务名称、联络人）查询考评任务； |
| 支持展示考核评价任务的任务名称、任务状态、任务时间、单位填报时间、创建单位、任务联络人及其联系方式、考评进度、任务附件、任务说明等信息； |
| 支持通过单位名称、单位任务状态查询考评任务的单位，支持统计待评分、已评分单位数，支持展示考评任务各单位的单位名称、所属区域、单位责任人、单位联系人、联系方式、单位任务状态等信息； |
| 考核指标 | 支持对考核评分任务评分； |
| 支持展示考核评分任务的任务名称、任务状态、任务时间、单位填报时间、创建单位、任务联络人及其联系方式、考评进度； |
| 态势感知升级服务 | 全链路网络安全监管平台 | ★支持监测并展示不同类别资产安全情况，包括云、网络、数据、应用、终端等，并支持下钻；**（提供功能截图证明材料）** |
| 支持统计监管的单位、系统、终端、数据资产数量； |
| 支持安全事件、风险隐患、网络攻击事件的展示，并支持下钻； |
| 支持展示单位安全考核排名情况、检查督查、制度规范、人员保障情况等； |
| 网络安全运营中心 | 支持按照本日、本周、本月、本年、近7天、近30天维度进行统计； |
| 支持政务云实例、骨干网设备、入网终端、应用系统、数据库的数据展示； |
| 支持展示制度规范，并支持预览；**（提供功能截图证明材料）** |
| 支持安全事件、风险隐患、网络攻击事件的展示； |
| 支持地图形式展示各区域安全告警和待办工单数量； |
| 全局安全态势 | 支持按照近七天、近一个月、近三个月、本周、本月、本年维度进行统计； |
| 支持单位、系统、资产、云平台、大数据平台、物联网、工业控制、移动APP的数据展示；**（提供功能截图证明材料）** |
| 支持安全事件、风险隐患、网络攻击事件的统计展示； |
| 支持安全区域和行业两个维度统计安全事件、风险隐患数量； |
| 支持区域通报情况、单位通报情况、行业通报情况的数据汇聚； |
| 支持预警中心、通报处置业务开展情况的数据统计；**（提供功能截图证明材料）** |
| 网络空间图谱 | 支持通过综合监管态势一张屏汇聚监管对象（如监管单位、关基设施、资产底数、驻点探针、分析流量、知识案例、威胁情报、安全大数据、联动城市）、监测成果（如安全事件、风险隐患、网络攻击）资产动态、黑客动态、实时通报、资产分布和网络攻击趋势等总体情况； |
| 支持在一张屏展示网络虚拟空间、单位地理空间、单位资产空间，直观反映三层之间的关联关系，支持将攻击行为从网络空间映射到地图空间，再到单位拓扑；**（提供功能截图证明材料）** |
| ★支持在三维地图展示安全事件，支持与后台事件调查功能联动，一键进行事件调查；**（提供功能截图证明材料）** |
| 支持大屏地图资产与后台信息发布一键联动，通过地图点击风险资产下发预警；（提供功能截图证明材料） |
| 支持对综合监管态势大屏展示内容进行自定义，支持自定义的内容不少于40种；资产统计维度包括行业分布、地域分布、开发框架等； |
| Web攻击态势 | 支持通过统一的可视化界面，集中监控并展示web类应用系统的被访问/攻击的安全态势； |
| 统计并展示当天网站集群的进出总流量、被访问/攻击总次数，在地图上进行动态可视化呈现； |
| 以列表形式统计以下内容并进行可视化呈现：网站区域访问量排行top5、访问IP排行top5、被攻击网站排行top50、攻击来源IP排行top10、攻击类型排行top10；（提供功能截图证明材料） |
| 实时刷新并滚动展示针对web业务的最新安全告警，包括攻击时间、地区/源IP、被攻击域名、被攻击URL、危险等级等信息； |
| 可点击钻取查看针对单个网站业务系统的攻击/访问信息； |
| 攻击者追踪溯源 | 支持通过独立的大屏界面，实现对攻击者的可视化溯源； |
| 支持统计并展示包括但不限于攻击者基本信息、攻击行为分析、相似IP分析、攻击取证信息、日志量、攻击趋势、攻击手段，攻击告警分布等信息； |
| 支持任意攻击者信息查询，支持最近24小时、最近7天，最近30天、本日、本周、本月周期进行可视化溯源分析； |
| 支持生成详细的攻击者溯源报告并能够一键导出； |
| IP资产威胁溯源 | 支持通过独立的大屏界面，实现对资产被攻击状况的可视化溯源分析； |
| 支持统计并展示包括但不限于资产基本信息、被攻击行为分析、相似资产分析、攻击来源分析、资产弱点、攻击取证信息、被访问趋势、日志量、被攻击手段、攻击源TOP等信息； |
| 支持最近24小时、最近7天，最近30天、本日、本周、本月周期选择进行可视化溯源分析，并支持任意资产被攻击信息查询； |
| 事件案例升级服务 | 支持通过攻击描述、标题查询相应事件案例；  |
| 支持对不同类型的事件案例进行快速搜索；  |
| 支持通过收藏按钮快速搜索本账号已收藏的事件案例；  |
| 支持对已有的事件案例进行编辑；  |
| 支持对已有的事件案例进行打标和编写批注操作；  |
| 支持手动录入已有的事件案例； |
| 数据对接 | ★要与数据管控平台进行对接，提供平台对接相关证明材料**；（所有数据对接费用均由供应商提供）** |
| 服务要求 | 一年 |

**12、风险评估服务**

|  |  |
| --- | --- |
| **技术指标** | **技术规格要求** |
| 总体要求 | 依据国家信息安全风险评估相关标准，结合信息安全整体需求及各系统具体应用特点，对信息系统定期开展信息安全风险评估； |
| 评估范围 | 10个信息系统； |
| 测评标准 | 委托的测评机构应具备 “检验机构”认可资质，且认可的能力范围包含上述信息安全风险评估标准； |
| 服务内容 | 依据省、市数据安全检查的要求，对重要业务系统进行风险评估，包括漏洞扫描（每年4次）、安全基线检查（每年4次）、渗透测试（每年1次）； |
| 输出物 | 出具《漏洞扫描报告》（4份）、《安全基线检查报告》（4份）、《渗透测试报告》（1份）、《风险评估报告》（1份）； |
| 服务要求 | 一年 |

**13、密码应用测评**

|  |  |
| --- | --- |
| **技术指标** | **技术规格要求** |
| 总体要求 | 依据《密码法》、《信息系统密码应用要求》、《商用密码应用安全性评估管理办法（试行）》等相关文件及标准要求，对5个三级系统进行密码应用测评； |
| 服务要求 | 依据标准（包括但不限于）如下：《信息系统密码应用基本要求》《信息系统密码测评要求》《信息系统密码应用测评过程指南》《信息系统密码应用高风险判定指引》《商用密码应用安全性评估量化评估规则》 |
| 测评内容 |  根据国家或行业相关标准，对信息系统完成商用密码应用安全性评估。信息系统商用密码应用安全性评估的内容（包括但不限于）： 根据用户单位信息系统的保护等级，并依据《信息系统密码应用基本要求》中条款要求，全面分析应用系统的安全保护措施与等级保护相应级别之间的差距，进行合规性分析，为系统等级保护加固整改提供客观依据，配合委托方督促集成商根据安全改进建议进行适度加固整改，具体测评内容如下：安全通用要求（密码算法、密码产品、密码技术、密码服务）；安全技术要求（物理和环境安全、网络和通信安全、设备和计算安全、应用和数据安全）；密钥管理要求；安全管理要求（制度、人员、实施、运行和应急）； |
| 服务成果 | 提交包括且不仅仅包括以下成果：《信息系统安全整改规划》《商用密码应用安全性评估报告》 |

**14、攻防演练及应急处置服务**

|  |  |
| --- | --- |
| **技术指标** | **技术规格要求** |
| 期限及频率 | 服务期内每年一次； |
| 服务范围 | 西湖区数据资源管理局系统； |
| 服务内容 | 在服务期内，为应对信息系统遇到突发的安全问题如：发生网络入侵事件、大规模病毒爆发、遭受拒绝服务攻击等，无法及时对该事件进行处理或解决的情况，提前针对此类事件进行应急方案的编制和演练，当此类事件发生时以便进行快速应对处置。 |
| 攻防演练服务要求 | 可选演练场景应包括但不限于：入侵系统攻击安全事件拒绝服务攻击安全事件病毒与木马攻击安全事件网站页面篡改安全事件数据库内部误操作可选演练内容应包括但不限于：信息篡改：模拟针对网站首页篡改事件的监控和处理（利用上传漏洞或者弱口令实施攻击）；拒绝服务：模拟从外部发起的针对网站的拒绝服务攻击事件的监控和处理（UD\CC等DDOS攻击工具）；恶意代码：模拟某恶意攻击者，利用系统的弱口令，利用windows共享管理服务（tcp/445），获得对服务器的控制权限；DNS劫持：模拟由于网站的域名解析管理账号存在弱口令，域名权威解析被篡改事件； |
| 应急处置服务要求 | 当出现安全事件时，必须及时进行响应，具体要求包括：1、技术人员必须在2小时内到达现场；2、对入侵事件进行分析，查找原因；3、抑制入侵事件的进一步发展，将事故的损害降低到最小化；4、排除安全隐患，消除安全威胁，协助恢复系统正常运作；5、提交应急响应报告及系统安全改进方案； |
| 服务成果 | 《安全事件应急响应报告》、《攻防演练总结报告》； |
| 服务能力要求 | ★服务商需自备应急处置工具箱1、任务管理（1）支持从应急处置管理平台下发处置任务，也可以新建应急处置任务；（2）处置任务的内容应包括事件描述、事件类型、事件级别、事发时间、事发单位、单位联系人、单位联系人电话、系统名称、保护等级、处置人员、资产信息等。2、攻击发现1）支持将漏洞验证工具检测结果与资产进行关联，并在工具箱上查看相应的扫描结果，提供界面截图；（2）支持数据库漏洞检测、系统漏洞检测、网站漏洞检测、病毒检测、木马检测；（3）支持自动导入功能，将验证工具集检测结果自动导入到工具箱，提供界面截图；3、处置对象（1）取证设备对象支持存储设备、边界设备、主机/服务器；（2）支持的日志文件类型包括IIS、Apache、Tomcat、Jboss、WebSphere、Weblogic；（3）支持添加对象事件线索，可以以手动填写、导入两种方式添加4、人工分析（1）支持以节点树的方式，对关键线索进行管理，并支持关键线索所有相关联IP及路径，提供界面截图；★（2）支持多条件对日志进行查询并显示，显示IP、IP地理信息、访问方法、访问时间、访问报文等，并支持从数据源、时间范围、后缀、IP等进行设置实现日志过滤，提供界面截图；（3）支持对日志进行不同颜色的标记，以标记关键日志；同时支持将日志添加入关键日志列表；（4）支持添加自定义线索；5、处置报告（1）资产安全漏洞应包含网站安全漏洞、网站恶意代码、操作系统及应用软件漏洞、数据库安全漏洞等安全风险；（2）应急处置情况应包含事件发生的过程、发生的原因及分析、事件如何处置及处置结果；★（3）报告应包含可疑IP及其物理地址；涉及可疑日志量及涉及关键日志量，提供界面截图； |
| 服务期 | 本次服务报价为一年服务费用，服务期为3年，合同按年签订，每年验收合格后续签合同。 |

**15、人员驻场服务**

|  |  |
| --- | --- |
| **技术指标** | **技术规格要求** |
| 总体要求 | 根据采购单位安排，针对西湖区电子政务网络安全、数据安全、PC终端外设等提供日常运维和技术保障服务，包括但不仅限于日常巡检、运行监控、故障处理等； |
| 服务人员 | 3名驻场服务人员，1人负责西湖区电子政务网络安全的运维工作；1人负责西湖区电子政务数据安全的运维工作；1人负责西湖区机关大院终端外设的运维工作； |
| 能力要求 | ★网络安全人员应熟悉主流的网络安全设备及技术原理，熟悉信息安全标准规范，具备CISP认证证书。 |
| 数据安全人员应具备数据安全相关工作能力，包括安全自查、部门安全检查、数据安全设施操作使用和日常维护等 |
| 终端外设运维人员应精通终端PC常见软硬件问题处理，熟悉终端故障排查，以及各类外设（打印机、复印件、扫描仪等设备）问题处置； |
| 服务时间 | 工作日5\*8小时，人员按照驻地（区政府大院）日常工作时间管理，并服从用户安排； |
| 服务期限 | 本次运维服务报价为一年服务费用，服务期为3年，合同按年签订，每年验收合格后续签合同； |
| 驻场人员到位后试用一个月，通过用户认可后由用户出具确认书，服务时间从驻场人员到位之日开始计算。如驻场人员试用未通过，服务单位应更换人员，直至人员通过试用并由用户出具确认书，服务时间从最后接替人员到位之日开始计算；服务期内人员变更时，新驻场人员同样需试用一个月，通过用户认可后由用户出具确认书； |
| 服务期 | 本次服务报价为一次服务费用，服务期为3年，合同按年签订，每年验收合格后续签合同。 |

**16、重保支持服务**

|  |  |
| --- | --- |
| **技术指标** | **技术规格要求** |
| 服务范围 | 重要会议、重大活动、重要事件期间，委派资深技术人员到场，为电子政务网络、安全、云计算平台等设备正常稳定运行提供保障，随时应急处理全区电子政务网络突发故障。人员须具备至少3年以上网络技术工作经验，服务时长：每年不少于27人天； |
| 服务期 | 本次服务报价为一年服务费用，服务期为3年，合同按年签订，每年验收合格后续签合同； |

**17、设备维保服务**

|  |  |
| --- | --- |
| **技术指标** | **技术规格要求** |
| 维保范围 | 1台天融信TSC-71232-WVS漏洞扫描系统；1台安恒DAS-A1000数据库审计设备；1套深信服SIP-1000－A600态势感知平台；以上设备需购买原厂商1年维保服务。 |
| 维保要求 | 保修期内提供7×24小时服务，在接到用户响应要求立即响应，4小时内到现场对故障进行处理，8小时内修复或解决；若硬件出现故障，要求中标单位及时免费修复或免费更换。服务内容包括故障处理、硬件维修、规则库升级（如有）等； |
| 其他 | ★投标时提供原厂商针对上述3台设备售后服务承诺函 |

**备注：**

1、硬件部分，投标人可参考上述表格提供的设备技术参数及配置，也欢迎优于本项目技术需求且性能与所明确要求相当的产品参加投标。

2、投标人应如实描述投标产品的主要指标偏离情况，若有偏离，只接受参数、性能优于招标要求的配置, 否则将被评标委员会技术扣分直至认定为投标无效。

**特别说明：**

1. 投标方及厂商必须保证所有投标产品（如光模块等）均为中华人民共和国境内合法销售的产品，并保证所有投标参数真实可信，同时承担以非法产品或虚假参数应标所带来的一切法律风险。中标单位提供的产品和服务符合国家相关安全规定及《浙江省信息技术服务外包安全管理规范》要求，如与国家相关安全规定及《浙江省信息技术服务外包安全管理规范》不符，，将做违约处理，并保留以诉诸相关法律进行处理的权利。

2.采购方会根据招标文件技术要求对中标单位所供产品进行功能及性能指标测试，如投标书中技术指标关键项说明与测试结果不符，将做违约处理，并保留以诉诸相关法律进行处理的权利。

3. 本项目用户方可以通过设备序列号在生产厂商官方网站或生产厂商400/800电话中进行验证，并可查询设备维保期限。

4. 投标清单中必须明确主机型号及配置各组件详细清单规格型号，无详细主机型号和组件清单型号的，视为不满足招标要求。

**5.为确保安全运维工作的及时性和故障处置效率，结合用户现有的安全设备情况，投标人应与主要安全设备原厂深信服、天融信、安恒建立快速协同机制，日常设备运维操作分别取得原厂深信服、天融信、安恒三家厂商授权和技术支持，配合现场运维工程师在最短的时间内解决问题。投标时提供三家厂商原厂技术支持授权函。**

6.凡是要求原厂维保的设备需提供原厂商针对本项目的服务承诺函原件，如中标单位拒绝或者无法提供承诺函原件，甲方将有权不予授予合同。（在投标时须上传原厂商服务承诺函原件扫描件或提供承诺书承诺响应以上要求）。

**五、项目实施要求**

1、中标方应在合同签订后**3个月内**完成本项目，需提供项目详尽的实施方案和进度表。

2、质量保证：

（1）投标产品必须是符合国家技术规范和质量标准的合格产品，满足采购人的使用需求，并具有可靠的售后服务体系，质量可靠、使用安全。

（2）投标人保证其提供的产品中所有预装和为本项目安装的软件均为具有合法版权或使用权的正版软件且无质量瑕疵，所提供硬件产品包括相关附件为相应硬件厂家原装正品，符合国家有关规定。投标人须保证所提供产品具有合法的版权或使用权，本项目采购的产品，如在本项目范围内使用过程中出现版权或使用权纠纷，应由中标人负责，采购人不承担责任。

（3）采购的开发软件也同时必须满足采购单位要求。

（4）在质保期内，如遇软件产品升级、改版，应免费提供更新、升级服务。

2、要求投标人提供的服务不得低于标准服务，即与投标产品制造厂商通过网站等对外公布的有效服务标准相一致（投标人不得另行制作网页）。在标准服务基础上，投标人还应达到以下标准：

（1）当投标货物发生非人为因素严重故障时，供应商应当免费在七日内将补充或者更换的货物运抵发生故障的货物所在地，由此产生的一切相关费用由供应商负担。

（2）质保期内所有因更换或修理设备或部件而导致设备停止运行的时间应从其质保期内扣除。

（3）供应商在质保期内安装的任何产品，必须是其投标产品制造厂商原产的或是经其认可的。

（4）所有的替代零配件必须是新的未使用和未经修复的，除非最终用户提供书面许可，否则不可使用此范围外的其他（非新的）配件。

（5） 供应商必须为维修和技术支持所未能解决的问题和故障提供正式的升级方案。

（6）在质保期内，供应商有责任解决所提供的投标设备和软件系统的任何问题，在质保期满后，当需要时，供应商仍须对因投标设备本身的固有缺陷和瑕疵承担相应责任。

3、对产品服务要求的有效响应将被视为投标人对其所投标产品的服务承诺，如果中标，须将服务承诺列入合同的产品服务条款。

4、投标人应在系统实施方案中描述具体的实施团队的组成、工作的内容、投入人员、项目进程表及采购人的配合等内容。在所有工作开展之前，中标方的实施人员应制定一套完整科学可行的实施方案，作为项目实施的总体计划和步骤。

5、培训要求

培训是项目顺利进行的保证。在项目的不同阶段要求提供相关的培训课程，面向系统开发和管理员、各级领导、系统操作人员等不同群体提供系统化、定制化和有针对性的培训。

6、售后服务要求

（1）投标人应具有完善的质保期内及质保期外的售后服务方案。

（2）硬件质保期不少于3年，安全设备和机房设施维保服务不少于1年，开发软件不少于1年质保期内提供免费的售后服务。

（3）所提供的技术服务至少为7×24小时支持维护服务，包括邮件、电话、远程维护、现场服务等方式。对故障1小时响应，4小时以内到现场，8小时以内解决问题；若硬件出现故障，要求中标单位及时免费修复或免费更换。

（4）投标人须具有本地化服务能力以及较强的专业技术队伍，在服务期内提供各方面服务，满足用户方所需的与应用软件相关的各类技术服务；

**六、验收要求**

文档的提交应覆盖以下内容，电子文档是成果不可分割的部分。要求如下文档：

1、项目实施前：需求分析报告；施工方案、项目实施计划；

2、项目实施期间：项目实施工作单、故障诊断及排除记录、项目实施过程中衍生的其它相关资料；

3、项目实施后：系统试运行和自测报告、故障诊断与排除手册、工作总结报告；

4、培训期间：培训计划、用户使用手册、管理员使用手册；

5、其他需要提交的材料。

**第四部分** **评标办法**

**评标办法前附表**

|  |  |  |  |
| --- | --- | --- | --- |
| 序号 | 评标标准 | 权重 | 投标文件中评标标准相应的商务技术资料目录 \* |
| 1 | 投标总体方案的功能实现及设计方案配置合理性等方面与项目对应需求的满足程度等 | 5 | （一）技术总体方案科学性和完整性 |
| 对用户现有的政务网络和数据安全现状理解是否全面、详尽、理解，在投标方案中对提供网络拓扑、网络设备和安全设备信息等情况介绍 | 8 |
| 投标人对项目安全风险、安全需求的理解，结合用户方网络现状、资源分布、安全防护现状等进行阐述，是否完整、切实可行 | 5 |
| 2 | 投标人对招标文件采购需求“四、采购内容及详细招标参数要求”第一至九项技术要求响应情况。带“★”的重要参数每负偏离1项扣1分；其他参数，每负偏离1项扣0.5分，扣完为止。注：①带“★”的重要参数均须提供相关的证明材料，不提供的按负偏离扣分；②其他参数未按要求提供相关证明材料的，不提供的按负偏离扣分。 | 12 | （二）功能需求的吻合程度 |
| 投标人对招标文件采购需求“四、采购内容及详细招标参数要求”所提供的软件（“数据安全管控分析服务”、“全链路安全监管升级服务”、“风险评估服务”、“密码应用测评”、“攻防演练及应急处置服务”）投标方案是否包含以下内容，方案需最大限度满足系统需求，方案与需求的契合度，对各功能细项进行详细论述。●“数据安全管控分析服务”、“全链路安全监管升级服务”和“攻防演练及应急处置服务”中带“★”的方案阐述是否合理、是否符合采购要求（13分）；●“风险评估服务”、“密码应用测评”、“数据安全管控分析服务”、“全链路安全监管升级服务”和“攻防演练及应急处置服务”中其他方案（指不带“★”的方案）阐述是否合理、是否符合采购要求（7分）。**注：不满足采购需求的或不提供投标方案论述的均不得分。** | 20 |
| 3 | ● 拟担任本项目经理和实施团队的专业素质、技术能力、经验等情况（提供人员资质、工作履历、参保证明等）（2分）； | 2 | （三）项目组人员素质情况 |
| ● 拟担任本项目驻场人员①人员数量是否满足招标文件要求3名驻场（1分）；②拟担任网络安全人员是否具备在有效期内的CISP认证证书（2分）；③人员驻场服务是否取得原厂深信服、天融信、安恒授权的技术支持，投标时提供原厂技术支持授权函，不提供此项不得分（2分）。 | 5 |
| ● 拟担任本项目重保支持服务人员①是否具备至少3年以上网络技术工作经验（2分）；②是否提供服务时长保证每年不少于27人天相关承诺（1分）； | 3 |
| 4 | 内容全面、措施有力，服务质量方面能够得到有效的保证，有明确的建设质量目标，质量保证措施，并具有详细可行的实施内容及工期保证和服务质保期保证等  | 2 | （四）质量保证措施 |
| 天融信TSC-71232-WVS漏洞扫描系统；安恒DAS-A1000数据库审计设备；深信服SIP-1000－A600态势感知平台；提供上述设备1年原厂商授权和技术支持的承诺函。每提供一个设备有效的售后维保承诺函得1分，共3分。 | 3 |
| 5 | 投标人项目组织实施方案的科学性、合理性、规范性和可操作性，包括系统集成、软件开发、试运行、测试、调优、系统管理培训、系统运行维护培训等内容，以及组织机构、工作时间进度表、工作程序和步骤、管理和协调方法、关键步骤的思路和要点等。  | 2 | （五）组织实施方案 |
| 6 | 投标人提出合理可行的培训计划、功能测试方案和验收方案。● 培训计划包括培训策略、培训方法、培训内容、培训时间地点、培训对象等（2分）；● 功能测试方案应包括测试工作准备、功能测试、性能测试的具体介绍（2分）；● 验收方案应包括验收组织、验收过程、验收成果物等关键描述（2分）。  | 6 | （六）培训、测试、试运行和验收 |
| 7 | ● 投标人提供的售后服务方案是否满足采购人的要求（1分）；● 投标人提供的①硬件②安全设备和机房设施维保服务③软件质保期限是否满足采购人的要求（3分）；● 质保期限及服务承诺的可行性、完整性以及服务承诺落实的保障措施等，系统出现问题后，供应商是否对故障1小时响应，4小时以内到现场，8小时以内解决问题（2分）。 | 6 | （七）售后服务保障能力 |
| 8 | 截止投标时间近三年以来投标人承担类似软件建设项目情况，结合已完工的案例和用户反映情况，**需提供合同复印件和付款凭证，每个有效案例得0.5分，共计1分。****（以签订时间为准，原件备查，采购机构在项目评审直至合同签订、履约期间，有权要求投标人出具投标文件中的主要业绩证明原件：如合同或用户验收报告等，予以确认其的真实性和有效性，如出现与事实不符等情况，将按照《中华人民共和国政府采购法》上报相关部门予以处罚**），是否有良好的工作业绩和履约记录等情况；**如投标人提供的合同复印件等实施项目证明材料与投标主体无关或违规转包分包的，评标委员会将进行扣分直至认定投标无效**。 | 1 | （十）类似项目建设的成功经验 |
| 10 | 系统演示及讲解（10分）：要求提供原型演示。不接受图片、PPT、Axure等高保真演示，否则演示不得分 | **针对数据安全管控分析服务的部分功能演示：****●共享与回流防护：**批量数据共享、回流、导出监管，发现违规回流项目空间、违规回流表、违规回流云账号等信息；异常回流告警（2分）；**●数据对接：**与杭州市数据管控平台对接，演示数据分类分级结果上报，工单流转（2分）；**●业务场景建模能力：**节点简单拖拽、连线对数据流转进行可视化拓扑配置；节点间的数据流转设置监控策略；基于数据流转拓扑进行监控，包括节点的访问量、流量、速率、延时、异常访问，及敏感数据访问监控；特定数据的全网流转拓扑自动梳理（2分）；**●资产识别梳理能力：**资产识别梳理能力：支持自动发现、手工录入方式梳理资产；以图表形式展示资产总量、各单位系统数量、系统所用资产数量等信息（2分）； **●规则引擎分析能力：**通过规则匹配等四大引擎编排内容，将来源、目标、标签等因子定义组合成规则；通过规则组合形成个性策略，对请求端信息及目标端返回的数据量、敏感度进行管控；数据安全场景规则自定义；变动告警阈值和告警生效节点演示（2分）。 | 10 | / |
| 11 | 有效投标报价的最低价作为评标基准价，其最低报价为满分；按［投标报价得分=（评标基准价/投标报价）\*10］的计算公式计算。评标过程中，不得去掉报价中的最高报价和最低报价。因落实政府采购政策需要进行价格调整的，以调整后的价格计算评标基准价和投标报价。 | 10 | / |

 \***备注：**投标人编制投标文件（商务技术文件部分）时，建议按此目录（序号和内容）提供评标标准相应的商务技术资料。

**一、评标方法**

**1.本项目采用综合评分法。**综合评分法，是指投标文件满足招标文件全部实质性要求，且按照评审因素的量化指标评审得分最高的投标人为中标候选人的评标方法。

**二、评标标准**

**2.** **评标标准：**见评标办法前附表。

**三、评标程序**

**3.1符合性审查。**评标委员会应当对符合资格的投标人的投标文件进行符合性审查，以确定其是否满足招标文件的实质性要求。不满足招标文件的实质性要求的，投标无效。

**3.2 比较与评价。**评标委员会应当按照招标文件中规定的评标方法和标准，对符合性审查合格的投标文件进行商务和技术评估，综合比较与评价。

**3.3汇总商务技术得分。**评标委员会各成员应当独立对每个投标人的商务和技术文件进行评价，并汇总商务技术得分情况。

**3.4报价评审。**

3.4.1投标文件报价出现前后不一致的，按照下列规定修正：

3.4.1.1投标文件中开标一览表(报价表)内容与投标文件中相应内容不一致的，以开标一览表(报价表)为准;

3.4.1.2大写金额和小写金额不一致的，以大写金额为准;

3.4.1.3单价金额小数点或者百分比有明显错位的，以开标一览表的总价为准，并修改单价;

3.4.1.4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。

3.4.1.5同时出现两种以上不一致的，按照3.4.1规定的顺序修正。修正后的报价按照财政部第87号令 《政府采购货物和服务招标投标管理办法》第五十一条第二款的规定经投标人确认后产生约束力。

3.4.2投标文件出现不是唯一的、有选择性投标报价的，投标无效。

3.4.3投标报价超过招标文件中规定的预算金额或者最高限价的，投标无效。

3.4.4评标委员会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，评标委员会应当将其作为无效投标处理。

3.4.5对于未预留份额专门面向中小企业的政府采购服务项目，以及预留份额政府采购服务项目中的非预留部分标项，对小型和微型企业的投标报价给予20%的扣除，用扣除后的价格参与评审。接受大中型企业与小微企业组成联合体或者允许大中型企业向一家或者多家小微企业分包的政府采购服务项目，对于联合协议或者分包意向协议约定小微企业的合同份额占到合同总金额30%以上的，对联合体或者大中型企业的报价给予6%的扣除，用扣除后的价格参加评审。组成联合体或者接受分包的小微企业与联合体内其他企业、分包企业之间存在直接控股、管理关系的，不享受价格扣除优惠政策。

**3.5排序与推荐。**采用综合评分法的，评标结果按评审后得分由高到低顺序排列。得分相同的，按投标报价由低到高顺序排列。得分且投标报价相同的并列。投标文件满足招标文件全部实质性要求，且按照评审因素的量化指标评审得分最高的投标人为排名第一的中标候选人。

多家投标人提供相同品牌产品（单一产品采购项目中的该产品或者非单一产品采购项目的核心产品）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；评审得分相同的，采取随机抽取方式确定，其他同品牌投标人不作为中标候选人。

**3.6编写评标报告。**评标委员会根据全体评标成员签字的原始评标记录和评标结果编写评标报告。评标委员会成员对需要共同认定的事项存在争议的，应当按照少数服从多数的原则作出结论。持不同意见的评标委员会成员应当在评标报告上签署不同意见及理由，否则视为同意评标报告。

**四、评标中的其他事项**

**4.1投标人澄清、说明或者补正。**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的内容需要投标人作出必要的澄清、说明或者补正的，评标委员会和投标人通过电子交易平台交换数据电文，投标人提交使用电子签名的相关数据电文或通过平台上传加盖公章的扫描件。给予投标人提交澄清、说明或补正的时间不得少于半小时，投标人已经明确表示澄清说明或补正完毕的除外。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。

**4.2投标无效。**有下列情形之一的，投标无效：

4.2.1投标人不具备招标文件中规定的资格要求的（投标人未提供有效的资格文件的，视为投标人不具备招标文件中规定的资格要求）；

4.2.2投标文件未按照招标文件要求签署、盖章的；

4.2.3采购人拟采购的产品属于政府强制采购的节能产品品目清单范围的，投标人未按招标文件要求提供国家确定的认证机构出具的、处于有效期之内的节能产品认证证书的；

4.2.4投标文件含有采购人不能接受的附加条件的；

4.2.5投标文件中承诺的投标有效期少于招标文件中载明的投标有效期的；

 4.2.6投标文件出现不是唯一的、有选择性投标报价的;

4.2.7投标报价超过招标文件中规定的预算金额或者最高限价的;

4.2.8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，未能按要求提供书面说明或者提交相关证明材料，不能证明其报价合理性的;

4.2.9投标人对根据修正原则修正后的报价不确认的；

4.2.10投标人提供虚假材料投标的；

 4.2.11投标人有恶意串通、妨碍其他投标人的竞争行为、损害采购人或者其他投标人的合法权益情形的；

4.2.12投标人仅提交备份投标文件，未在电子交易平台传输递交投标文件的，投标无效；

## 4.2.13 投标文件不满足招标文件的其它实质性要求的；

4.2.14法律、法规、规章（适用本市的）及省级以上规范性文件（适用本市的）规定的其他无效情形。

**5.废标。**根据《中华人民共和国政府采购法》第三十六条之规定，在采购中，出现下列情形之一的，应予废标：

5.1符合专业条件的供应商或者对招标文件作实质响应的供应商不足3家的；

5.2出现影响采购公正的违法、违规行为的；

5.3投标人的报价均超过了采购预算，采购人不能支付的；

5.4因重大变故，采购任务取消的。

废标后，采购机构应当将废标理由通知所有投标人。

**6.修改招标文件，重新组织采购活动。**评标委员会发现招标文件存在歧义、重大缺陷导致评标工作无法进行，或者招标文件内容违反国家有关强制性规定的，将停止评标工作，并与采购人、采购机构沟通并作书面记录。采购人、采购机构确认后，将修改招标文件，重新组织采购活动。

**7.重新开展采购。**有政府采购法第七十一条、第七十二条规定的违法行为之一，影响或者可能影响中标结果的，依照下列规定处理：

7.1未确定中标供应商的，终止本次政府采购活动，重新开展政府采购活动。

7.2已确定中标供应商但尚未签订政府采购合同的，中标结果无效，从合格的中标候选人中另行确定中标供应商；没有合格的中标候选人的，重新开展政府采购活动。

7.3政府采购合同已签订但尚未履行的，撤销合同，从合格的中标候选人中另行确定中标供应商；没有合格的中标候选人的，重新开展政府采购活动。

7.4政府采购合同已经履行，给采购人、供应商造成损失的，由责任人承担赔偿责任。

7.5政府采购当事人有其他违反政府采购法或者政府采购法实施条例等法律法规规定的行为，经改正后仍然影响或者可能影响中标结果或者依法被认定为中标无效的，依照7.1-7.4规定处理。

**第五部分 拟签订的合同文本**

合同编号：

**政府采购合同参考范本**

**（服务类）**

**第一部分 合同书**

项目名称：

甲方：

乙方：

签订地：

签订日期： 年 月 日

根据《中华人民共和国政府采购法》和《中华人民共和国民法典》、地方有关法律、法规和政策，在平等、自愿、协商一致的基础上，就甲方（中共杭州市西湖人大常委会）委托乙方（经评审最终确定的成交供应商）对杭州市西湖区电子政务整体安全体系改造提升（2022）项目订立本合同。

**1、 定义**

1. “合同”即由甲乙方双方签订的合同格式中的文件，包括所有的附件、附录和组成合同部分的所有其他文件。

合同将由杭州市西湖区数据资源管理局（以下简称甲方）与经评审最终确定的成交供应商（以下简称乙方）结合本项目具体情况协商后签订。以下为采购单位提出涉及乙方的主要条款，投标人在投标文件中应对其进行确认或拒绝。如投标人在其投标文件中未做拒绝或提出修改要求的，采购单位将视作认同。

2. “合同价格”系指根据合同规定，在供应商全面正确地履行合同义务时，采购单位应支付给供应商的款项。

3.“服务”系指招标文件规定供应商须承担的安装、调试、技术协助、校准、培训以及其它类似的义务。

4. “甲方”系指通过采购接受合同及服务的杭州市西湖区数据资源管理局。

5. “乙方”系指经评审最终确定的成交供应商。

6. “现场”系指将要进行系统安装和运转的地点。

7. “验收”系指采购人依据国家有关规定接受合同所依据的程序和条件。

**2、 适用范围**

本合同条款适用与本次采购活动。项目实施范围详见附件——投标文件和投标文件及补充文件、承诺书等。

**3．项目开发与要求**

3.1乙方必须在合同签订后10天内进一步优化需求分析、概要设计、详细设计，并细化系统建设计划、目标任务书和测试验收方案，向采购人提供上述文档并需经采购人审查通过。

3.2合同签订后3个月内完成项目的全部建设并通过初步验收，进入试运行（试运行1个月）。

3.3试运行内完成培训及相关的修改，建立完善的系统运维体系，经终验合格，正式交付使用，进入维保服务。

3.4乙方对所提供的开发产品、技术开发和服务等拥有合法的占有和处置权，并对涉及项目的所有内容可能侵权行为指控负责，保证不伤害甲方的利益。在法律范围内，如果出现文字、图片、商标和技术等侵权行为而造成的纠纷和产生的一切费用，甲方概不负责，由此给甲方造成损失的，乙方要承担相应后果，并负责赔偿。乙方为执行本项目合同而提供的技术资料等归甲方所有。

3.5乙方在投标文件中所列的开发产品等应与实际安装实施的产品完全一致，并提供相关证明。如发现产品与投标报价书等资料不符，甲方有权更换，其一切后果及费用由乙方承担。如发现不符合功能性能要求、质量要求等情况由乙方负责重新开发或补足，并不得影响建设开发工期。

3.6乙方必须按照本项目进度推进实施，按照项目需求、国家技术规范和质量标准实施项目开发和系统集成。

3.7该项目的应用软件成果由甲方与乙方共同所有。但乙方对甲方提供的业务资料、技术资料应严格保密，不得扩散。

**4．项目实施**

4.1甲方提供项目所需的数据信息支持和必要场地。

4.2乙方项目实施人员须服从甲方管理人员管理。乙方项目实施人员必须遵守现场的各项规章制度。

4.3乙方应根据项目情况提供硬件送货安装、系统集成、软件开发、安装调试计划，项目实施进度计划，经甲、乙双方共同确定后作为双方共同执行的合同条款，乙方应按计划完工交付验收，若超过计划完工日15天以上的按超期处罚。

**5．系统维护与保修**

5.1 乙方对甲方提供操作维护、管理等培训。

5.2 乙方提供 7×24小时售后技术支持服务**（软硬件产品质保期3年，安全设备维保1年，其它按照招标需求执行)**，从验收合格之日起计算。

5.3 维护期内，乙方须根据系统运行情况进行不定期的检测与调优，每半年对系统进行一次总体检测。

5.4 乙方在每次服务完成后，须向用户提交相关文档，内容包括起因、响应、过程、结果、今后注意事项等各部分。

**6．验收**

甲方对所供系统进行最终验收。甲方将组织有关专家对系统进行验收。如果发现与合同中要求不符，乙方须承担由此发生的一切损失和费用，并接受相应的处罚。验收合格后，甲乙双方共同签署验收报告，一式二份，一份交甲方留存，一份由乙方用作结算凭证。项目验收有关费用由中标单位承担。

**7、项目价款及调整**

本招标项目采取固定总价承包，未经甲方认可，不得以任何理由予以变更，除以下列明的价款调整和计算方法之外，所有费用包干，不予调整。乙方应按甲方提供的要求报价，缺项、漏项和产品偏离视作报价已包含在其它子项中，不予以调整。允许乙方对招标文件提供的技术方案在投标价格不增加且能扩大使用功能的前提下，可提出合理化建议或优化方案，做出其优越性、先进性等详细说明。

**8．支付**

本次项目合同总价为人民币 （￥ 元），采用分期付款方式：

|  |  |  |  |
| --- | --- | --- | --- |
| 付款期数 | 付款大写金额（元） | 付款小写金额（元） | 付款时间 |
| 一 |  |  | 合同签订后10个工作日内，进行详细的需求调研，进一步优化概要设计、详细设计，并细化系统建设计划、目标任务书和测试验收方案，向甲方提供上述文档并需经甲方审查通过。乙方凭甲方签字盖章的支付通知书向甲方办理合同总价40%的款项支付手续。 |
| 二 |  |  | 合同签订后**3个月**内完成所有设备、材料的到货、安装调试、系统集成、软件开发、培训测试等，初验合格后进入试运行后10个工作日内，乙方凭甲方签字盖章的支付通知书、初验报告向甲方办理合同总价40%的款项支付手续。 |
| 三 |  |  | 系统正常运转**1个月**后（试运行1个月），提交全部报告材料，并通过最终验收，出具项目终验报告。乙方凭甲方签字盖章的支付通知书、发票复印件、终验报告向甲方办理合同总价20%的货款结算手续。 |

**9**. **履约保证金缴纳及退付**

9.1 签订合同后3个工作日内，中标人（乙方）须向采购人（甲方）缴纳不超过政府采购合同总额1％的履约保证金，缴纳金额: （￥元）。采购人在项目验收合格后，若无质量和服务等问题，在5个工作日内将履约保证金原额（无息）归还中标人；

**9.2 甲方根据杭州市政府采购网公布的供应商履约评价情况减免履约保证金。乙方履约验收评价总分为100分的，甲方免收履约保证金。**

9.3履约保证金可以用支票、汇票、本票或者银行、保险公司出具的保函等非现金形式交纳。

**10．延期交付与核定损失额**

如果乙方在正常情况下未能按合同规定的时间按期交付使用或未能按合同规定履行其义务，乙方将承担相应后果，甲方有权从履约保证金中取得补偿。

**11．不可抗力**

签约双方任一方由于不可抗力事故的影响而不能执行合同时，履行合同的期限应予以延长。不可抗力事故系指甲乙双方在缔结合同时所不能预见的，并且它的发生及其后果无法避免和无法克服的事故。

**12. 乙方的责任与义务**

12.1 根据投标文件的承诺向甲方委派项目负责人、技术负责人和专业技术人员。

12.2 在履行本合同义务的期间，应运用合理的技能，认真、勤奋工作。

12.3 在本合同期内或合同终止后，未征得有关方同意，不得泄露与本项目、本合同有关的技术、资料等，不得以任何形式侵害甲方的知识产权。

12.4 负责本系统项目建设及整体联动，负责处理好与其他项目实施单位的协调。

12.5 项目建设有关事项包括：项目规划、设计标准、规范和使用功能要求，向甲方的建议权；

12.6 项目设计中的技术问题，按照安全和优化的原则，提出建议，并向甲方提出书面报告。如果由于拟提出的建议会提高项目造价，或延长工期，应当事先取的甲方的同意；

12.7 项目实施组织设计和技术方案，按照保质量、保工期和降低成本的原则，向甲方提出书面报告。如果由于拟提出的建议会提高项目造价，或延长工期，应当事先取得甲方的同意。

12.8乙方须保证所提供软件系统是拥有合法版权的产品，符合国家有关规定。能提供技术及备件支持。乙方须保证所提供产品具有合法的版权或使用权，如在本项目范围内使用过程中出现版权或使用权纠纷，应由乙方负责，甲方不承担责任。

**13. 甲方的责任与义务**

13.1 甲方应当主要负责项目建设的所有外部关系的联系与协调，为乙方工作提供良好的外部条件。

13.2 甲方应当按合同条款双方约定的内容和时间，向乙方提供与项目建设有关的项目资料等。

13.3 甲方应当按合同条款约定的时间就乙方书面提交并要求做出决定的一切事宜做出书面决定。逾期应视为甲方同意。

13.4 甲方应授权一名熟悉本项目情况、能迅速做出决定的项目代表，负责与乙方联系。更换代表，要提前通知乙方。

13.5 甲方有与乙方订立补充合同的签订权。

13.6 甲方有对项目规模、设计标准、规范和设计使用功能要求的认定权，以及对项目建设、设计变更的审批权。

13.7 甲方有权要求乙方提交工作月度报告及专项报告等。

**14. 合同生效、变更和终止**

14.1 本合同经甲乙双方法定代表人或其委托人签字盖章，并且乙方向甲方缴纳合同约定金额的履约保证金或建议免收履约保证金，合同在政采云平台备案后生效。至合同期止。

**14.2.合同转让和分包:本项目不允许分包。**

14.3 在乙方的责任期即合同的有效期内，如因甲方的原因，导致项目建设进度的推迟或延误而超过约定的日期，甲乙双方应协商，重新约定相应延长的合同期。因乙方的责任，导致项目建设进度的推迟或延误而超过约定的日期按违约责任处罚。

14.4 在合同签订后，实际情况发生变化，使得乙方不能全部或部分执行项目时，乙方应当立即通知甲方。该项目的完成时间应延长。当恢复执行项目时，是否需增加时间用于恢复执行，由双方协商确定。

14.5 当事人一方要求变更或解除合同时，应当在30天前通知对方，因变更或解除合同使一方遭受损失的，除依法可以免除责任的外，应由责任方负责赔偿。变更或解除合同的通知或协议应当采取书面形式，协议未达成之前，原合同仍然有效。

**15. 违约责任**

15.1乙方必须在整个项目安装调试开通全部完成后约定时间内，会同甲方及有关部门共同按有关规范验收，如因产品质量和项目实施质量问题，不能按期验收或验收不合格，乙方应负责返工所造成的经济损失。由此而造成推迟交货的时间按超期天数计算，每超过一天乙方按本项目总价款的2‰赔偿甲方的经济损失。如因甲方原因造成不能按期完工，工期相应顺延。

15.2 如在合同规定的工期内，达不到项目规定的技术指标，乙方应当承担违约责任。承担方式和违约金额如下：超期30天内，每天扣合同金额的0.5‰；累计超期30天，甲方有权终止执行合同，并没收履约保证金。

15.3 如因乙方原因达不到合格等级的，则必须无条件返工至合格，并全额没收履约保证金。

15.4因乙方原因造成采购单位其他系统不能正常运行，酿成重大事故（正常工作日系统中断一天或一天以上）的，将承担全部法律责任，并赔偿经济损失，赔偿金额最高为项目总价的50%。

15.5 履行本合同的过程中，确因在现有水平和条件下难以克服的技术困难，导致部分或全部失败所造成的损失，风险责任由乙方全部承担。

15.6 因不可抗力导致合同不能全部或部分履行，甲、乙双方协商解决。

**16.安全责任与处罚**

16.1**网络数据安全责任**。乙方应按照《网络安全法》、《数据安全法》、《个人信息保护法》的要求，履行网络和数据安全相关责任和义务，项目涉及人员需签订《保密承诺书》，对驻场服务人员进行背景审查。乙方应当采取技术措施和其他必要措施，确保网络和数据安全，防止信息泄露、毁损、丢失。在发生或者可能发生信息泄露、毁损、丢失的情况时，应当立即采取补救措施，并在第一时间告知甲方。未经甲方允许，乙方不得对建设、运营、运维的信息系统、应用、数据库等私开账户、擅自更改权限等操作，严禁乙方多名工作人员共用账号，严禁使用弱密码。乙方应加强网络安全风险监测，制定应急预案，完善应急机制。确保第一时间检测发现，第一时间应急处置，第一时间向甲方报告。

16.2**网络数据安全处罚**。由于乙方原因，受到国家级、省级、市级安全问题通报或造成特别重大事故的，每次扣除合同款5万元、3万元、1万元，乙方不及时处置安全事件、隐患的,每次扣除合同款1万元。乙方派驻的驻场人员未按照甲方工作要求进行出勤的，每出现1人次扣除500元。收到国家、省、市通报后，乙方应及时解决并递交书面整改报告给甲方，若乙方未根据整改报告按期整改的，每次扣除合同款1万元。以上扣除总额不超过合同的20%。

**17.项目质量**

17.1 乙方保证按ISO9000系列标准或相应的质量管理和质量保证体系，对项目安装、调试、检验等各个环节进行严格的质量和质量控制。

17.2 乙方须严格按设计方案和国家现行项目实施验收规范有关规定，精心组织安装、调试、记录、检验。

17.3 项目的质量、技术标准如在招标文件和投标文件中无相应说明，则按中华人民共和国有关部门颁布的最新的国家或专业（部）标准或相应的国际标准执行。没有国家或专业（部）标准的，按企业标准执行。

17.4 项目竣工验收：应按设计方案、技术交底、会审纪要、设计变更通知单、国家和部颁发的有关规范和质量检验评定标准、相关的国际标准为依据，并有相关专业测试单位出具相应的测验结论报告。

17.5 项目实施过程中应严格做好安全防范措施，如乙方项目实施人员在施工中违反操作规定造成人员伤亡事故或施工现场防范措施设置不明造成人员伤害事故，一切责任均有乙方负责。

**18. 争议处理**

18.1 合同在履行过程中发生争议时，甲方与乙方及时协商解决。协商不成时，依法向人民法院起诉。

18.2 对于因违反或终止合同而引起的损失、损害的赔偿，由甲方与乙方友好协商解决，经协商仍未能达成一致的，依法向人民法院起诉。

**19. 其他**

19.1 本合同（□是 □否）为可融资合同（若为可融资合同，则甲方必须将采购资金支付到合同中指定的融资银行及收款账号，开户银行： 账号： ）。关于中小企业信用融资事项可登录杭州市政府采购网 “中小企业融资系统”专栏进行查询。

19.2 未经过甲方的书面同意，乙方不得转让其应履行的合同项下的义务，和将部分合同项下的义务分包给其他单位完成。

19.3 乙方不得参与可能与合同规定的与甲方的利益相冲突的任何活动。

19.4 乙方人员在甲方场地工作时，应遵守甲方相关规章、制度。

19.5 本合同任何一方给另一方的通知，都应以书面或电传/传真/电报的形式发送，而另一方应以书面形式确认并发送到对方明确的地址。

19.6 合同履行期内甲乙双方均不得随意变更或解除合同。合同若有未尽事宜，需经双方共同协商，订立补充协议，补充协议与本合同有同等法律效力。

19.7 招标文件[编号：XHZFCG-2022-G-42]、投标文件及评标过程中形成的文字资料、询标纪要均作为本合同的组成部分，具有同等效力。

19.8 本合同经甲乙双方法定代表人或其委托人签字盖章，并且乙方向甲方缴纳合同约定金额的履约保证金或建议免收履约保证金，合同在政采云平台备案后生效。

19.9 本合同一式伍份，甲方、乙方各执贰份，采购机构执壹份。

19.10 适用法律：本合同应按照中华人民共和国的法律进行解释。

 19.11 以上是合同的主要条款，合同条款包括但不止于以上条款（如安全生产责任状以及廉政合同等）。

甲方（盖章）： 乙方（盖章）：

法定代表人： 法定代表人：

或受委托人（签字）： 或受委托人（签字）：

联系人： 联系人：

地址： 地址：

电话： 电话：

传真： 传真：

开户银行： 开户银行：

帐号： 帐号：

签 约 地：

 签约日期： 年 月 日

**第六部分 应提交的有关格式范例**

**资格文件部分**

**目录**

（1）符合参加政府采购活动应当具备的一般条件的承诺函……………（页码）

（2）联合协议………………………………………………………………（页码）

（3）落实政府采购政策需满足的资格要求………………………………（页码）

（4）本项目的特定资格要求………………………………………………（页码）

 **一、 符合参加政府采购活动应当具备的一般条件的承诺函**

杭州市西湖区数据资源管理局、杭州市西湖区政府采购中心：

我方参与杭州市西湖区电子政务整体安全体系改造提升（2022）项目【招标编号：XHZFCG-2022-G-42】政府采购活动，郑重承诺：

（一）具备《中华人民共和国政府采购法》第二十二条第一款规定的条件：

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和专业技术能力；

4、有依法缴纳税收和社会保障资金的良好记录；

5、参加政府采购活动前三年内，在经营活动中没有重大违法记录；

6、具有法律、行政法规规定的其他条件。

（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、政府采购严重违法失信行为记录名单。

（三）不存在以下情况：

1、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政府采购活动的；

2、为采购项目提供整体设计、规范编制或者项目管理、监理、检测等服务后再参加该采购项目的其他采购活动的。

投标人名称(电子签名)：

 日期： 年 月 日

**二、联合协议（如果有）**

**[以联合体形式投标的，提供联合协议（附件5）；本项目不接受联合体投标或者投标人不以联合体形式投标的，则不需要提供）]**

**三、落实政府采购政策需满足的资格要求**

（根据招标公告落实政府采购政策需满足的资格要求选择提供相应的材料；未要求的，无需提供）

**A**.专门面向中小企业，服务全部由符合政策要求的中小企业（或小微企业）承接的，提供相应的中小企业声明函（附件7）。

**四、本项目的特定资格要求**

（根据招标公告本项目的特定资格要求提供相应的材料；未要求的，无需提供）

**商务技术文件部分**

**目录**

（1）投标函…………………………………………………………………………………（页码）（2）授权委托书或法定代表人（单位负责人、自然人本人）身份证明………（页码）

（3）分包意向协议…………………………………………………………………………（页码）

（4）符合性审查资料………………………………………………………………………（页码）

（5）评标标准相应的商务技术资料……………………………………………………（页码）

（6）投标标的清单…………………………………………………………………………（页码）

（7）商务技术偏离表………………………………………………………………………（页码）

（8）政府采购供应商廉洁自律承诺书…………………………………………………（页码）

**一、投标函**

杭州市西湖区数据资源管理局、杭州市西湖区政府采购中心：

我方参加你方组织的杭州市西湖区电子政务整体安全体系改造提升（2022）项目【招标编号：XHZFCG-2022-G-42】招标的有关活动，并对此项目进行投标。为此：

1、我方承诺投标有效期从提交投标文件的截止之日起 天（不少于90天），本投标文件在投标有效期满之前均具有约束力。

2、我方的投标文件包括以下内容：

2.1资格文件：

2.1.1承诺函；

2.1.2联合协议（如果有)；

2.1.3落实政府采购政策需满足的资格要求（如果有）；

2.1.4本项目的特定资格要求（如果有）。

2.2 商务技术文件：

2.2.1投标函；

2.2.2授权委托书或法定代表人（单位负责人）身份证明；

2.2.3分包意向协议（如果有）；

2.2.4符合性审查资料；

2.2.5评标标准相应的商务技术资料；

2.2.6商务技术偏离表；

2.2.7政府采购供应商廉洁自律承诺书；

2.3报价文件

2.3.1开标一览表（报价表）。

3、我方承诺除商务技术偏离表列出的偏离外，我方响应招标文件的全部要求。

4、如我方中标，我方承诺：

4.1在收到中标通知书后，在中标通知书规定的期限内与你方签订合同；

4.2在签订合同时不向你方提出附加条件；

4.3按照招标文件要求提交履约保证金；

4.4在合同约定的期限内完成合同规定的全部义务。

5、其他补充说明: 。

投标人名称（电子签名）：

 日期： 年 月 日

注：按本格式和要求提供。

**二、授权委托书或法定代表人（单位负责人、自然人本人）身份证明**

**授权委托书（适用于非联合体投标）**

杭州市西湖区数据资源管理局、杭州市西湖区政府采购中心：

现委托 （姓名）为我方代理人（身份证号码： ，手机： ），以我方名义处理杭州市西湖区电子政务整体安全体系改造提升（2022）项目【招标编号：XHZFCG-2022-G-42】政府采购投标的一切事项，其法律后果由我方承担。

 委托期限：自 年 月 日起至 年 月 日止。

 特此告知。

 投标人名称(电子签名)：

 签发日期： 年 月 日

 **授权委托书（适用于联合体投标）**

杭州市西湖区数据资源管理局、杭州市西湖区政府采购中心：

现委托 （姓名）为我方代理人（身份证号码： ，手机： ），以我方名义处理杭州市西湖区电子政务整体安全体系改造提升（2022）项目【招标编号：XHZFCG-2022-G-42】政府采购投标的一切事项，其法律后果由我方承担。

 委托期限：自 年 月 日起至 年 月 日止。

 特此告知。

联合体成员名称(电子签名/公章)：

联合体成员名称(电子签名/公章)：

……

 日期： 年 月 日

**法定代表人、单位负责人或自然人本人的身份证明（适用于法定代表人、单位负责人或者自然人本人代表投标人参加投标）**

身份证件扫描件：

|  |
| --- |
| 正面： 反面： |

 投标人名称(电子签名)：

 日期： 年 月 日

**三、分包意向协议**

[**中标后以分包方式履行合同的，提供分包意向协议(附件6)；采购人不同意分包或者投标人中标后不以分包方式履行合同的，则不需要提供。**]

**四、符合性审查资料**

|  |  |  |  |
| --- | --- | --- | --- |
| **序号** | **实质性要求** | **需要提供的符合性审查资料** | **投标文件中的****页码位置** |
| 1 | 投标文件按照招标文件要求签署、盖章。 | 需要使用电子签名或者签字盖章的投标文件的组成部分 | 见投标文件第 页 |
| 2 | 采购人拟采购的产品属于政府强制采购的节能产品品目清单范围的，投标人按招标文件要求提供国家确定的认证机构出具的、处于有效期之内的节能产品认证证书。 | 节能产品认证证书**（本项目拟采购的产品不属于政府强制采购的节能产品品目清单范围的，无需提供）** | 见投标文件第 页 |
| 3 | 投标文件中承诺的投标有效期不少于招标文件中载明的投标有效期。 | 投标函 | 见投标文件第 页 |
| 4 | 投标文件满足招标文件的其它实质性要求。 | 招标文件其它实质性要求相应的材料（**“▲” 系指实质性要求条款，招标文件无其它实质性要求的，无需提供**） | 见投标文件第 页 |

注：按本格式和要求提供。

**五、评标标准相应的商务技术资料**

**（按招标文件第四部分评标办法前附表中“投标文件中评标标准相应的商务技术资料目录”提供资料。）**

**六、投标标的清单**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **序号** | **名称** | **服务范围（品牌）** | **服务要求（规格型号）** | **服务时间（规格配置详细说明）** | **服务标准** | **备注（如果有）** |
| 1 |  |  |  |  |  |  |
| 2 |  |  |  |  |  |  |
| …… |  |  |  |  |  |  |

**注：按本格式和要求提供。**

**七、商务技术偏离表**

|  |  |  |  |
| --- | --- | --- | --- |
| **序号** | **招标文件章节及具体内容** | **投标文件章节及具体内容** | **偏离说明** |
| 1 |  |  |  |
| 2 |  |  |  |
| …… |  |  |  |

投标人保证：除商务技术偏离表列出的偏离外，投标人响应招标文件的全部要求

注：按本格式和要求提供。

**八、政府采购供应商廉洁自律承诺书**

杭州市西湖区数据资源管理局、杭州市西湖区政府采购中心：

我单位响应你单位项目招标要求参加投标。在这次投标过程中和中标后，我们将严格遵守国家法律法规要求，并郑重承诺：

一、不向项目有关人员及部门赠送礼金礼物、有价证券、回扣以及中介费、介绍费、咨询费等好处费；

二、不为项目有关人员及部门报销应由你方单位或个人支付的费用；

三、不向项目有关人员及部门提供有可能影响公正的宴请和健身娱乐等活动；

四、不为项目有关人员及部门出国（境）、旅游等提供方便；

五、不为项目有关人员个人装修住房、婚丧嫁娶、配偶子女工作安排等提供

好处；

六、严格遵守《中华人民共和国政府采购法》《中华人民共和国招标投标

法》《中华人民共和国民法典》等法律法规，诚实守信，合法经营，坚决抵制各种违法违纪行为。

如违反上述承诺，你单位有权立即取消我单位投标、中标或在建项目的建设资格，有权拒绝我单位在一定时期内进入你单位进行项目建设或其他经营活动，并通报市财政局。由此引起的相应损失均由我单位承担。

投标人名称（电子签名）：

日期： 年 月 日

注：按本格式和要求提供。

**报价文件部分**

**目录**

（1）开标一览表（报价表）………………………………………………………（页码）

一、开标一览表（报价表）

杭州市西湖区数据资源管理局、杭州市西湖区政府采购中心：

按你方招标文件要求，我们，本投标文件签字方，谨此向你方发出要约如下：如你方接受本投标，我方承诺按照如下开标一览表（报价表）的价格完成杭州市西湖区电子政务整体安全体系改造提升（2022）项目【招标编号：XHZFCG-2022-G-42】的实施。

**开标一览表（报价表）(单位均为人民币元)**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **序号** | **名称** | **具体服务（品牌规格型号）** | **数量（单位：项）** | **单价（元）** | **总价（元）** | **服务年限（质保年限）** |
| 1 |  |  |  |  |  |  |
| 2 |  |  |  |  |  |  |
| 3 |  |  |  |  |  |  |
| …… |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
| **投标报价（小写）** |  |
| **投标报价（大写）** |  |

**注：**

▲**1、更新网络边界、网络通信、计算环境等基础设施，搭建公共数据平台安全技术体系，升级迭代现有数据管控平台，实现全链路监管体系的报价不得超过546.6万元整；攻防演练及应急处置服务的报价不得超过3万元整/年，服务期3年；3名人员驻场服务的报价不得超过45万元整/年，服务期3年；网络重保支持服务的报价不得超过5万元整/年，服务期3年；**

**攻防演练及应急处置服务、人员驻场服务及网络重保支持服务的服务期均为3年，合同按年签定，每年验收合格后续签合同。**

**注：其中硬件质保期不少于3年，安全设备和机房设施维保服务不得少于1年，软件不少于1年（含）7×24小时免费售后技术服务。**

**2、投标人需按本表格式填写，否则视为投标文件含有采购人不能接受的附加条件，投标无效；**

3、有关本项目实施所涉及的一切费用均计入报价。**采购人将以合同形式有偿取得货物或服务，不接受投标人给予的赠品、回扣或者与采购无关的其他商品、服务**，**不得出现“0元”“免费赠送”等形式的无偿报价，否则视为投标文件含有采购人不能接受的附加条件，投标无效；采购内容未包含在《开标一览表（报价表）》名称栏中，投标人不能作出合理解释的，视为投标文件含有采购人不能接受的附加条件的，投标无效。**

4、特别提示：采购机构将对项目名称和项目编号，中标供应商名称、地址和中标金额，主要中标标的名称、服务范围、服务要求、服务时间、服务标准等予以公示。

5、符合招标文件中列明的可享受中小企业扶持政策的投标人，请填写中小企业声明函。注：投标人提供的中小企业声明函内容不实的，属于提供虚假材料谋取中标、成交，依照《中华人民共和国政府采购法》等国家有关规定追究相应责任。

供应商名称（电子签名）：

 日期： 年 月

**政府采购支持中小企业信用融资相关事项通知**

为贯彻落实中央、省、市关于支持民营经济健康发展有关精神，发挥政府采购在促进中小企业发展中的政策引导作用，缓解中小企业融资难、融资贵问题，杭州市财政局、

中国银保监会浙江监管局、杭州市地方金融监督管理局、杭州市经济和信息化局制定《杭州市政府采购支持中小企业信用融资管理办法》。相关事项通知如下：

**一、适用对象**

凡已在浙江政府采购网上注册入库，并取得杭州市政府采购合同的中小企业供应商（以下简称“供应商”），均可申请政府采购信用融资。

**二、相关信息获取方式**

市财政局在杭州市政府采购网上建设信用融资模块，并与“浙里办”浙江政务服务平台对接，推进政府采购中标成交信息、合同信息等信息资源共享，鼓励各银行采用线上融资模式，将银行业务系统与信用融资模块对接，实现供应商“一次也不跑”，同时提供相关的服务支持，做好协调工作。

**三、　政府采购信用融资操作流程：**

（一）线上融资模式：

　　1.供应商根据合作银行提供的方案，自行选择金融产品，并办理开户等手续；

　　2.供应商中标后，可通过杭州市政府采购网或“浙里办”测算授信额度；

　　3.采购合同签订后，供应商在杭州市政府采购网或“浙里办”向合作银行发出融资申请；

　　4.审批通过后，在线办理放贷手续。

　　（二）线下融资模式：

　　1.供应商根据合作银行提供的方案，自行选择金融产品，向合作银行提出信用资格预审，并办理开户等手续；

　　2.采购合同签订后，供应商在杭州市政府采购网或“浙里办”向合作银行发出融资申请；

　　3.合作银行在信用融资模块受理申请后，供应商提供审批材料。合作银行应对申请信用融资的供应商及备案的政府采购合同信息进行核对和审查；

　　4.审批通过后，合作银行应按照合作备忘录中约定的审批放款期限和优惠利率及时予以放款。

## （三）杭州e融平台申请融资

## 供应商通过杭州e融平台政采贷专区，自行选择金融产品，按规定手续办理贷款流程。

**四、注意事项**

1、对拟用于信用融资的政府采购合同，供应商在签订合同时应当在合同中注明融资银行名称及账号，作为在该银行的唯一收款账号。

2、供应商弄虚作假或以伪造政府采购合同等方式违规获取政府采购信用融资，或不及时还款，或出现其他违反本办法规定情形的，按融资合同约定承担违约责任；涉嫌犯罪的，移送司法机关处理。

# 附件

**附件1：**

**残疾人福利性单位声明函**

本单位郑重声明，根据《财政部 民政部 中国残疾人联合会关于促进残疾人就业政府采购政策的通知》（财库〔2017〕 141号）的规定，本单位为符合条件的残疾人福利性单位，且本单位参加\_\_\_\_\_\_单位的\_\_\_\_\_\_项目采购活动提供本单位制造的货物（由本单位承担工程/提供服务），或者提供其他残疾人福利性单位制造的货物（不包括使用非残疾人福利性单位注册商标的货物）。

本单位对上述声明的真实性负责。如有虚假，将依法承担相应责任。

 投标人名称（电子签名）：

 日 期：

**附件2：质疑函范本及制作说明**

**质疑函范本**

一、质疑供应商基本信息

质疑供应商：

地址： 邮编：

联系人： 联系电话：

授权代表：

联系电话：

地址： 邮编：

二、质疑项目基本情况

质疑项目的名称：

质疑项目的编号： 包号：

采购人名称：

采购文件获取日期：

三、质疑事项具体内容

质疑事项1：

事实依据：

法律依据：

质疑事项2

……

四、与质疑事项相关的质疑请求

请求：

签字(签章)： 公章：

日期：

**质疑函制作说明：**

1.供应商提出质疑时，应提交质疑函和必要的证明材料。

2.质疑供应商若委托代理人进行质疑的，质疑函应按要求列明“授权代表”的有关内容，并在附件中提交由质疑供应商签署的授权委托书。授权委托书应载明代理人的姓名或者名称、代理事项、具体权限、期限和相关事项。

3.质疑供应商若对项目的某一分包进行质疑，质疑函中应列明具体分包号。

4.质疑函的质疑事项应具体、明确，并有必要的事实依据和法律依据。

5.质疑函的质疑请求应与质疑事项相关。

6.质疑供应商为自然人的，质疑函应由本人签字；质疑供应商为法人或者其他组织的，质疑函应由法定代表人、主要负责人，或者其授权代表签字或者盖章，并加盖公章。

**附件3：投诉书范本及制作说明**

**投诉书范本**

一、投诉相关主体基本情况

投诉人：

地 址： 邮编：

法定代表人/主要负责人：

联系电话：

授权代表： 联系电话：

地 址： 邮编：

被投诉人1：

地 址： 邮编：

联系人： 联系电话：

被投诉人2

……

相关供应商：

地 址： 邮编：

联系人： 联系电话：

二、投诉项目基本情况

采购项目名称：

采购项目编号： 包号：

采购人名称：

代理机构名称：

采购文件公告:是/否 公告期限：

采购结果公告:是/否 公告期限：

三、质疑基本情况

投诉人于 年 月 日,向 提出质疑，质疑事项为：

采购人/代理机构于 年 月 日,就质疑事项作出了答复/没有在法定期限内作出答复。

四、投诉事项具体内容

投诉事项 1：

事实依据：

法律依据：

投诉事项2

……

五、与投诉事项相关的投诉请求

请求：

签字(签章)： 公章：

日期：

**投诉书制作说明：**

1.投诉人提起投诉时，应当提交投诉书和必要的证明材料，并按照被投诉人和与投诉事项有关的供应商数量提供投诉书副本。

2.投诉人若委托代理人进行投诉的，投诉书应按照要求列明“授权代表”的有关内容，并在附件中提交由投诉人签署的授权委托书。授权委托书应当载明代理人的姓名或者名称、代理事项、具体权限、期限和相关事项。

3.投诉人若对项目的某一分包进行投诉，投诉书应列明具体分包号。

4.投诉书应简要列明质疑事项，质疑函、质疑答复等作为附件材料提供。

5.投诉书的投诉事项应具体、明确，并有必要的事实依据和法律依据。

6.投诉书的投诉请求应与投诉事项相关。

7.投诉人为自然人的，投诉书应当由本人签字；投诉人为法人或者其他组织的，投诉书应当由法定代表人、主要负责人，或者其授权代表签字或者盖章，并加盖公章。

**附件4：业务专用章使用说明函**

杭州市西湖区数据资源管理局、杭州市西湖区政府采购中心

我方 (投标人全称)是中华人民共和国依法登记注册的合法企业，在参加你方组织的杭州市西湖区电子政务整体安全体系改造提升（2022）项目项目【招标编号：XHZFCG-2022-G-42】投标活动中作如下说明：我方所使用的“XX专用章”与法定名称章具有同等的法律效力，对使用“XX专用章”的行为予以完全承认，并愿意承担相应责任。

特此说明。

投标单位（法定名称章）：

 日期： 年 月 日

**附：**

投标单位法定名称章（印模） 投标单位“XX专用章”（印模）

**附件5：联合协议**

**（以联合体形式投标的，提供联合协议；本项目不接受联合体投标或者投标人不以联合体形式投标的，则不需要提供）**

（联合体所有成员名称）自愿组成一个联合体，以一个投标人的身份参加杭州市西湖区电子政务整体安全体系改造提升（2022）项目【招标编号：XHZFCG-2022-G-42】投标。

一、各方一致决定，（某联合体成员名称）为联合体牵头人，代表所有联合体成员负责投标和合同实施阶段的主办、协调工作。

二、所有联合体成员各方签署授权书，授权书载明的授权代表根据招标文件规定及投标内容而对采购人、采购机构所作的任何合法承诺，包括书面澄清及相应等均对联合投标各方产生约束力。

三、本次联合投标中，分工如下：

（联合体成员1）承担的工作和义务为： ；

（联合体成员2）承担的工作和义务为： ；

……

四、联合体成员中小企业合同份额。

1、（联合体成员X,……）提供的服务由小微企业承接，其合同份额占到合同总金额 %以上。**（****未预留份额专门面向中小企业采购的采购项目，以及预留份额中的非预留部分采购包，接受联合体投标的，联合协议约定小微企业的合同份额占到合同总金额30%以上的，对联合体报价给予6%的扣除。供应商拟享受以上价格扣除政策的，填写有关内容。）**

2、中小企业合同金额达到 %，小微企业合同金额达到 %。**（要求以联合体形式参加的项目或采购包，供应商按招标文件第一部分招标公告申请人的资格要求中规定的联合协议中中小企业、小微企业合同金额应当达到的比例要求填写。）**

五、如果中标，联合体各成员方共同与采购人签订合同，并就采购合同约定的事项对采购人承担连带责任。

六、有关本次联合投标的其他事宜：

1、联合体各方不再单独参加或者与其他供应商另外组成联合体参加同一合同项下的政府采购活动。

2、联合体中有同类资质的各方按照联合体分工承担相同工作的，按照资质等级较低的供应商确定资质等级。

3、本协议提交采购人、采购机构后，联合体各方不得以任何形式对上述内容进行修改或撤销。

联合体成员名称(电子签名/公章)：

 日期： 年 月 日

注：按本格式和要求提供。

**附件6：分包意向协议**

（**中标后以分包方式履行合同的，提供分包意向协议；采购人不同意分包或者投标人中标后不以分包方式履行合同的，则不需要提供。**）

（投标人名称）若成为杭州市西湖区电子政务整体安全体系改造提升（2022）项目【招标编号：XHZFCG-2022-G-42】的中标供应商，将依法采取分包方式履行合同。（投标人名称）与（所有分包供应商名称）达成分包意向协议。

一、分包标的及数量

（投标人名称）将 XX工作内容 分包给（分包供应商1名称），（分包供应商2名称），具备承担XX工作内容相应资质条件且不得再次分包；

## ……

二、分包供应商中小企业合同份额

1、（分包供应商X,……）提供的服务全部由小微企业承接，其合同份额占到合同总金额 %以上。**（未预留份额专门面向中小企业采购的采购项目，以及预留份额中的非预留部分采购包，允许分包的，分包意向协议约定小微企业的合同份额占到合同总金额30%以上的，对大中型企业的报价给予6%的扣除。供应商拟享受以上价格扣除政策的，填写有关内容。）**

2、中小企业合同金额达到 %，小微企业合同金额达到 %。**（要求合同分包形式参加的项目或采购包，供应商按招标文件第一部分招标公告申请人的资格要求中规定的分包意向协议中中小企业、小微企业合同金额应当达到的比例要求填写。）**

三、分包工作履行期限、地点、方式

四、质量

五、价款或者报酬

六、违约责任

七、争议解决的办法

八、其他

中小企业合同金额达到 %，小微企业合同金额达到 % 。 投标人名称(电子签名)：

分包供应商名称：

……

 日期： 年 月 日

**附件7：中小企业声明函**

**中小企业声明函（服务）**

本公司（联合体）郑重声明，根据《政府采购促进中小企业发展管理办法》（财库﹝2020﹞46 号）的规定，本公司（联合体）参加 杭州市西湖区数据资源管理局 的 杭州市西湖区电子政务整体安全体系改造提升（2022）项目 采购活动，工程的施工单位全部为符合政策要求的中小企业（或者：服务全部由符合政策要求的中小企业承接）。相关企业（含联合体中的中小企业、签订分包意向协议的中小企业）的具体情况如下：

1. （标的名称），属于 （采购文件中明确的所属行业） ；承建（承接）企业为 （企业名称） ，从业人员 人，营业收入为 万元，资产总额为 万元属于 （中型企业、小型企业、微型企业） ；

以上企业，不属于大企业的分支机构，不存在控股股东为大企业的情形，也不存在与大企业的负责人为同一人的情形。

本企业对上述声明内容的真实性负责。如有虚假，将依法承担相应责任。

投标人名称（电子签名）：

日 期：

**从业人员、营业收入、资产总额填报上一年度数据，无上一年度数据的新成立企业可不填报。**

 注：

1、填写要求：①“标的名称”、“采购文件中明确的所属行业”依据招标文件第二部分投标人须知前附表中“采购标的及其对应的中小企业划分标准所属行业”的指引**逐一填写，不得缺漏**；②从业人员、营业收入、资产总额填报上一年度数据，无上一年度数据的新成立企业可不填报；③中型企业、小型企业、微型企业等3种企业类型，结合以上数据，依据《中小企业划型标准规定》（工信部联企业〔2011〕300号）确定；④投标人提供的《中小企业声明函》与实际情况不符的或者未按以上要求填写的，中小企业声明函无效，不享受中小企业扶持政策。声明内容不实的，属于提供虚假材料谋取中标、成交的，依法承担法律责任。

2、符合《关于促进残疾人就业政府采购政策的通知》（财库〔2017〕141号）规定的条件并提供《残疾人福利性单位声明函》（附件1）的残疾人福利性单位视同小型、微型企业；根据《关于政府采购支持监狱企业发展有关问题的通知》（财库[2014]68号）的规定，投标人提供由省级以上监狱管理局、戒毒管理局（含新疆生产建设兵团）出具的属于监狱企业证明文件的，视同为小型和微型企业。