项目编号：310112000230227114456-12019262

上海市闵行区卫建委医卫云运维服务项目（2023 运维）

单一来源

采购文件

采购单位：上海市闵行区卫生健康信息中心

地　　址：友东路 358 号 3 号楼 3 楼

联 系 人：**机构管理员**

联系方式：**021-64985537**

集中采购机构：闵行区政府采购中心

地　　址：闵行区秀文路 600 号 713、716 室

联 系 人：**洪晓明**

联系方式：**33882619**

目 录

第一章　单一来源采购邀请

根据《中华人民共和国政府采购法》、《政府采购非招标采购方式管理规定》、《中华人民共和国政府采购法实施条例》规定，经相关审批程序核准，现就下列项目向包 1：中国电信股份有限公司上海分公司。行单一来源采购：

一、**项目编号：**3101120002302271144 56-12019262

二、**采购内容及数量**

包号	包名称	数量	单位	预算金额（元）	简要规格描述或包基本概况介绍	最高限价（元）	备注
1	上海市闵行区卫建委医卫云运维服务项目（2023运维）	1		6594316.00	上海市闵行区卫建委医卫云运维服务项目（2023运维）	6594316.00	

三、**合格供应商的资格要求**

1、符合《中华人民共和国政府采购法》第二十二条的规定

2、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

无

上海市闵行区卫建委医卫云运维服务项目（2023运维）资格审查要求包 1

序号	类型	审查要求	要求说明	项目级/包级

四、**单一来源采购的时间和地点：**

时间：2023-05-09 14:00:00

地点：闵行区秀文路 600 号主楼 336 会议室

供应商应准时派全权代表出席（全权代表应当是供应商的在职正式职工，

并携带身份证等有效证明出席）。

五、单一来源采购文件的获取：

供应商报名后自行下载（http://www.zfcg.sh.gov.cn/）。

六、报名方式：

本项目实行网上报名，不接受现场报名。供应商登录上海市政府采购网（http://www.zfcg.sh.gov.cn/）进行报名。

七、单一来源采购保证金：（本项目不适用）

[投标保证金收款账户（金额、开户行、户名、账号等）]

供应商应于 将保证金以网银、汇票、电汇、转帐支票方式（不接受以现金支票、现金及个人转账方式交纳的保证金），保证金若以电汇、网银方式交纳的,请将电汇底单、网银电脑打印凭证写上所投项目名称、编号、供应商联系人、联系电话。

第二章　供应商须知

前附表

序号	内　　容　　及　　要　　求
1	项目名称及数量：详见《单一来源采购邀请》
2	是否允许进口产品：不允许进口产品
3	转包与分包：否；联合投标：不允许。
4	演示时间：不进行演示
5	单一来源采购响应文件份数： （1）电子版投标文件按电子投标相关要求提供； （2） 纸质文件两份，为电子版投标文件的打印版； **备注：第（2）条不作为本项目实质性要求。**
6	采购结果公示：采购结果经采购人确认后，采购中心将于2个工作日内在上海市政府采购网上公告成交结果，并向成交供应商发出成交通知书。
7	签订合同时间：成交通知书发出后30日内。
8	付款方式：国库集中支付（采购人自行支付），详见各标项的资信及商务要求表。
9	*1、投标人（响应人，报价人）资格审查、符合性检查、评标委员会的评审等均以投标文件为准，投标人（响应人，报价人）在上海政府采购网中另行上传的资料应与上传的电子版投标文件中相关资料保持一致，若出现不一致或缺漏的，**均以上传的电子版投标文件为准**。 *2、投标人（响应人，报价人）在上海政府采购网录入的投标报价，应与上传的电子版投标文件中开标一览表的报价一致（最后报价以最终提交的书面承诺为准）。**因上海政府采购网网上投标录入系统的报价目前无法修改，报价不一致的，将由评标委员会审核后在报价评审阶段做无效报价处理。**
10	解释：单一来源采购文件的解释权属于上海市闵行区政府采购中心**采购中心。**

一、总　则

单一来源是指采购人为了从某一特定供应商处采购货物、工程和服务，采购中心组织具有相关经验的专业人员与供应商商定合理的成交价格并保证采购项目质量的采购方式。

（一） 适用范围

仅适用于本次单一来源采购文件中所叙述的货物及服务采购。

（二）定义

1.“采购机构”系指组织本次采购的上海市闵行区政府采购中心。

2.“供应商”系指向采购中心提交单一来源采购响应文件的单位。

3.“采购人” 系指委托采购中心采购本次项目的国家机关、事业单位和团体组织。

4.“产品”系指供应商按单一来源采购文件规定，须向采购人提供的一切设备、保险、税金、备品备件、工具、手册及其它有关技术资料和材料。

5.“服务”系指单一来源采购文件规定供应商须承担的安装、调试、技术协助、校准、培训、技术指导以及其他类似的义务。

6.“项目”系指供应商按单一来源采购文件规定向采购人提供的产品和服务。

（三）谈判费用

3.1 无论采购结果如何，响应人自行承担所有与参加本项目有关的全部费用。

(四)采购文件的说明

4.1 采购文件用以阐明所需货物及服务、协商程序、技术规格及要求和合同条款（格式）。

4.2 本采购文件的组成：

第一章　单一来源采购邀请

第二章　供应商须知

第三章　采购内容

第四章　采购合同主要条款指引

第五章 评审办法

第六章　响应文件格式及附件

4.3 采购文件的澄清及修改

4.3.1 响应人对采购文件如有疑点，应在递交响应文件截止时间 3 日前以书面形式（包括信函、传真）送达闵行区政府采购中心，闵行区政府采购中心将收到的澄清要求以书面形式予以答复，逾期的澄清要求一律不予作答。

4.3.2 在递交响应文件截止前，采购人可主动地或依据响应人要求澄清的问题而修改采购文件，并以书面形式通知获得采购文件的响应人，对方在收到该通知后应立即作收到回函确认。

4.3.3 修改文件将构成采购文件的一部分，对响应人有约束力。

(五)响应文件的编制

5.1 响应文件的语言及计量

5.1.1 响应人与闵行区政府采购中心就有关采购的所有书面来往函电均使用简体中文书写，且使用 **A4**纸格式。

5.1.2 本采购文件所叙述的时间、价格，若无特殊说明均以北京时间和人民币作考量。

5.1.3 凡电子招标的投标文件中，需要投标人提供证明文件及资料的，均为原件的扫描件（包括图片格式），外部的证明资料无需加盖投标人公章。

5.2 响应文件的构成

5.2.1 响应人提交的响应文件必须包含以下内容，要求有页码及目录：

商务部分：

（1） 响应函

（2） 响应人声明函

（3） 法定代表人授权书

（4） 报价一览表

（5） 各分项报价一览表、详细货物（服务）一览表

（6） 廉政承诺书

（7） 响应人身份证明

（8） 财务状况及税收、社会保障资金缴纳情况声明函

（9） 中小企业声明函（若有）

（10） 残疾人福利性单位的证明资料（若有）

（11） 三年内无重大违法记录的书面声明

（12） 商务条款偏离表

（13） 在“信用中国”网站(www.creditchina.gov.cn)和中国政府采购网(www.ccgp.gov.cn)查询的信用记录结果

（14） 采购文件规定的其它资格证明文件

（15） 采购文件要求的其他内容以及响应人认为需加以说明的其他内容

技术部分：

（1）对本项目总体要求的理解。

（2）工艺说明、质量指标及材料选型说明

（3）项目的实施进度、质量等保证措施

（4）验收方案

（5）售后服务的内容和措施

（6）履行合同所配备的管理、技术人员清单

（7）节能环保产品证明或证书（若有）

（8）质量保证书(若有)、节能产品承诺书（若有）

（9）采购文件要求的其他内容以及响应人认为需加以说明的其他内容

响应文件装帧要求

纸质版响应文件必须装订成册。响应文件的装订应牢固、不易拆散和换页。

5.3 响应文件的份数

5.3.1 见本采购文件前附表的要求。

6.响应有效期

6.1 采购文件确定的响应有效期为 90 天,以递交响应文件截止时间之日起始计。

6.2 在特殊情况下,闵行区政府采购中心可以书面通知已递交响应文件的响应人延长应谈有效期，响应人收到闵行区政府采购中心的延期通知后必须在第一时间作书面回函确认。

6.3 延长响应有效期内，本项目采购当事人受响应有效期限制的所有权利和义务均延长至新的响应有效期。

(六)无效标的情形

在采购时，如发现下列情形之一的，单一来源采购响应文件将被视为无效：

1、供应商最终报价超出预算的；

2、最终报价明显高于其市场报价或低于成本价且不能合理说明原因并提供证明材料的；

3、供应商未能提供合格的资格文件；

4、与单一来源采购文件有重大偏离的；

5、采购响应文件未有效授权；

6、不符合法律、法规和本单一来源采购文件规定的其他实质性要求的。

(七)协商与成交

9. 协商程序

9.1 闵行区政府采购中心按本采购文件载明的时间、地点组织单一来源采购人员与响应人进行协商，商定合理的成交价格并保证采购项目的质量。

9.2 单一来源采购人员编写协商情况记录。

10. 成交

10.1 根据协商情况记录确认成交供应商后，由闵行区政府采购中心向成交供应商发出《中标（成交）通知书》，《中标（成交）通知书》一经发出即发生法律效力。

10.2《中标（成交）通知书》发出后，成交供应商放弃成交的，应当承担法律责任。

11. 签订合同

11.1 采购人和成交供应商应当自《中标（成交）通知书》发出之日起 30 天内签订合同。

11.2 采购文件、成交供应商的响应文件和协商情况记录等，均为签订经济合同的依据。

（八）其他要求或说明

12.1 本采购文件的约束条件与采购人授予成交供应商合同中法律有效期同时截止。

12.2 响应人在获得采购文件并进行协商后，即表示无条件接受本采购文件所有条款的约束。

12.3 本采购文件的最终解释权归上海市闵行区政府采购中心。

第三章　采购内容

上海市闵行区卫健委医卫云运维服务项目
(2023 运维)
采购需求
（单一来源）

采购单位：上海市闵行区卫生健康信息中心

背景
闵行区医卫云已经在 2021 年 10 月验收完成上线后，目前已经承载 200 多个应用系统，未来将持续为闵行区卫健委、区内综合医院、社区医院等医疗机构提供服务。故本项目基于现有的医卫云，优先考虑提供产品及服务的服务商、优先考虑提供云平台服务供应商，实现医卫云平台能够稳定、便捷的对居民提供服务。
项目预算及分项报价上限

序号	服务名称	描述	批复金额（元）
1	基础设施-物理托管	整机柜租用 单价 42000 数量 2 个	84000
2	基础设施-网络资源	互联光纤 单价 960 元，数量 20 公里	19200
3	基础设施-网络资源	应用负载均衡 单价 240 元，数量 289 每 IP	69360
4	基础设施-网络资源	安全交换区 单价 9600 元，数量 36 每 IP	345600
5	基础设施-计算资源	CPU 单价 180 元，数量 3825 核	688500
6	基础设施-计算资源	内存 单价 180 元，数量 18750G	3375000
7	基础设施-存储资源	应用存储空间 单价 960 元，数量 342.55TB	328848
8	基础设施-存储资源	高性能数据库存储 单价 1800 元，数量 120.9TB	217620
9	基础设施-存储资源	数据备份 单价 960 元，数量 342.55TB	328848
10	基础设施-存储资源	数据归档 单价 2100 元，数量 1 套	2100
11	信息安全技术-安全 防护	网络访问控制 单价 20000 元，数量 2 租户	40000

12	信息安全技术-安全 防护	入侵防御 单价 1800 元，数量 2 租户	3600
13	信息安全技术-用户安全	用户管理 单价 6600 元，数量 2 租户	13200
14	信息安全技术-用户安全	用户身份认证 单价 6600 元，数量 2 租户	13200
15	信息安全技术服务-安全接入服务	VPN 接入 单价 7200 数量 2 租户	14400
16	信息安全技术服务-安全管理服务	网络行为安全审计服务 单价 2300 数量 2 套	4600
17	信息安全技术服务-安全管理服务	安全隐患分析服务 单价 4600 数量 2 套	9200
18	信息安全技术-安全管理	数据库审计 单价 5400 元，数量 60 实例	324000
19	信息安全技术-安全扫描	常规安全漏洞扫描 单价 690 数量 2 次	1380
20	信息安全技术-安全扫描	系统上线安全扫描 单价 690 元，数量 2VM/次	1380
21	信息安全技术-网站防护	在线防护 WAF 单价 4140 元，数量 2 套	8280
22	信息安全技术-网站防护	网页防篡 单价 7000 元，数量 2 套	14000
23	信息安全技术服务-密码安全服务	密码安全服务 单价 518400 数量 1 套	518400
24	灾备-数据级	单价 169600 元，数量 1 套	169600
合计			6594316

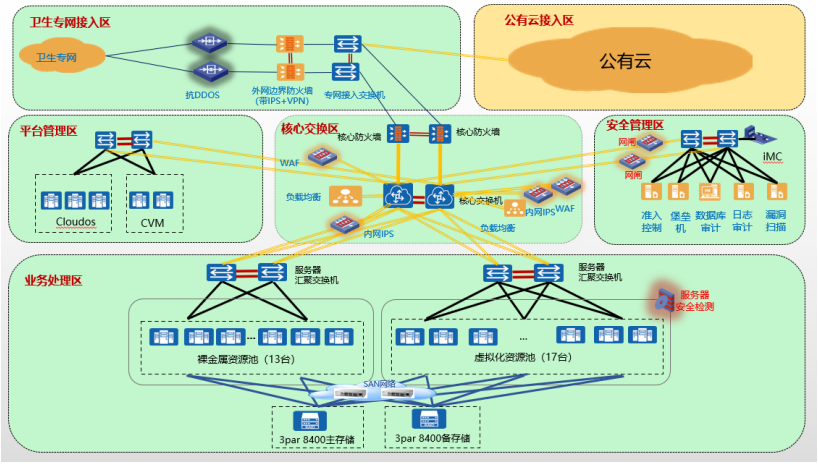
服务需求和技术总体要求

项目现状

闵行区卫健委医卫云平台现有在运行业务系统和数据库数量已超过 220 个,目前医卫云平台运行状况良好。2021-2022 年还陆续新增闵行区“互联网+护理服务”、闵行区全民健康区域管理平台、闵行区卫健委信息化项目管理系统等应用。随着就医人员配套在线信息化服务需求的增加,用户数据量和业务访问量逐步增加，业务系统需要的基础设施资源量也随之增加。

现有网络拓扑现状

目前闵行区医卫平台的拓扑如下图，业务处理区承载着闵行区卫健委超过 95%的业务系统，平台管理区、核心交换区、安全管理区、卫生专网接入区共同支撑着整个医卫云平台的安全、管理、数据交互等。



项目目标

闵行区医卫云平台采用云计算技术，打造基于混合云服务全新架构平台，能够满足各项业务应用连续性、稳定性、安全性的要求。该云平台能够提供丰富的云服务，包括但不限于云主机、物理机、云硬盘、负载均衡、防火墙、数据库、云管理平台等服务，满足不同业务使用需求。其中云管理平台能够实现本地虚拟和物理资源池、公有云资源池、运营和运维的统一管理，即“一云多池”：充分利用云计算资源弹性伸缩、快速部署的优势，实现资源供给多样化，各资源池之间逻辑隔离，根据实际业务灵活调整，快速响应业务需求，可以简便、迅速地支持医疗卫生系统现有应用的扩展和新应用的建设。

本项目计划继续通过购买中国电信云服务，集中部署、虚拟化技术动态按需分配信息化资源，提高资源的利用效率，降低建设成本和管理维护成本，节约财政资金投入，提高信息化效率，顺利通过等保三级认证。从而实现闵行区医疗卫生信息资源的统一维护与共享，为提高诊疗水平、优化诊疗流程、便民惠民服务等提供更好的技术支撑。

招标内容

总体采购

区域名称	服务/服务对象	具体运维服务内容
云 DC 网络边界	专线出口交换机，出口防火墙，DDoS 清洗，DDoS 检测，应用负载均衡，WAF	DDos 流量清洗、防火墙、应用负载均衡 289 个 IP、安全交换区 36 个 IP、在线防护 WAF 2 套等
云核心交换区	入侵防御，WAF，核心防火墙，数据库审计、网络访问控制	WAF、IPS 防入侵、防病毒、数据库审计 60 例、网络访问控制数量 2（租户）、入侵防御数量 2（租户）、安全漏扫 2 次；
计算资源池（含裸金属服务器资源）	虚拟化服务器	虚拟资源：CPU 达到 3825 核，虚拟机内存配置达到 18750G；
存储区（含裸金属服务器资源）	存储，备份存储及备份软件	主存储：403TB（15% SSD 硬盘，85% 机械盘） 备存储：403TB（15% SSD 硬盘，85% 机械盘） 数据归档：1 套
管理区	云管理服务器，虚拟化软件，数据中心云管理软件，堡垒主机，双因素认证，安全扫描、网页防篡、主机配置核查，主机安全，管理防火墙	堡垒机、双因素认证、安全扫描 2VM/次、网页防篡 2 套、VPN 接入 2（租户）、安全隐患分析服务 2 套、网络行为安全审计服务 2 套、统一管理软件等
用户安全	用户管理、用户身份证认证	用户管理数量 2（租户）、用户身份证认证数量 2（租户）
专线	卫生网接入专线	1000M*2 线（卫生网接入私有云）数量共 20

		公里
密码安全	密码安全服务	密码安全服务 1 套
灾备软件	数据库灾备软件	数据级
物理托管	整机柜租用	2 个

私有云
综合考虑应用、数据、网络的安全，要求满足等保 2.0 三级要求。私有云用于承载闵行区医卫云平台所有核心区域的业务及应用、与卫生专网、公有云区域的互联互通。具体要求如下。
计算资源
▲云平台的计算资源池（含裸金属服务器资源）中 CPU 资源 3825 核数，内存资源 18750G。其中虚拟化计算资源池中 CPU 资源 3341 核数，内存资源 11518G；裸金属服务器资源为 CPU484 核，内存资源 7232G。裸金属服务器具体配置信息如下：
新数据中心和区域平台配置 2 台裸金属服务器，单台配置为 2 路 10 核、64G 内存、2*1.8T 硬盘；新公卫和 40 库配置 4 台裸金属服务器，单台配置为 4 路 12 核、1536G 内存、2*1.8T 硬盘；影像云配置 2 台裸金属服务器，单台配置为 4 路 12 核，256G 内存、2*1.8T 硬盘；医联体 4 路配置 2 台裸金属服务器，单台配置为 4 路 12 核，128G 内存、2*1.8T 硬盘；医联体 2 路配置 3 台裸金属服务器，单台配置为 2 路 10 核，64G 内存、2*1.8T 硬盘。
▲云主机 CPU 内存要求支持 1:1、1:2、1:4、1:8 等典型规格实例。
▲可在 48 核 256GB 范围内定义任意规格的云主机。
▲每个虚拟机都可以安装独立的操作系统，为获得良好的兼容性，操作系统需要支持包括 Windows、Linux 的多个版本：Windows 2008 R2、Windows 2012 R2、Windows 2019、CentOS 6 到 8 版本、RHEL5 到 8 版本、Ubuntu 14 到 20 版本，并且支持国产操作系统包括：红旗 linux、中标麒麟、中标普华等。以上操作系统若官方发布更新的，也纳入支持范围。
▲云主机的系统盘可支持配置普通云盘或 SSD 高性能云盘，可自定义系统盘大小。
控制台支持云主机的开机、关机、重启、强行关机、挂载云硬盘、卸载云硬盘等操作。
▲支持私有镜像服务，用户可制作自己的镜像文件并上传到云主机，以实现灵活管理、批量部署，用户制作的私有镜像仅限该用户使用。
可展示云主机的 CPU、内存、系统盘、数据盘的资源利用率。
虚拟机可以实现物理机的全部功能，如具有自己的资源（内存、CPU、网卡、存储），可以指定单独的 MAC 地址等。
▲支持虚拟机的备份，支持直接将虚拟机备份到磁盘，并支持生成全新虚拟机的方式进行恢复。
▲支持虚拟机卡死及蓝屏的检测功能并实现自动重启，无需人工干预减少运维工作量。
支持虚拟机的 HA 功能。当物理服务器发生故障时，该物理服务器上的所有虚拟机，可以在集群之内的其它物理服务器上重新启动，保障业务连续性。
▲支持对平台虚拟机的精细化权限管理，可根据单个虚拟机开关机、打开控制台、删除等操作设定不同的权限，管理员也可以根据用户需求合理分配权限。
存储资源
▲存储资源支持不少于 403TB 空间，支持容量盘与 SSD 盘两种云硬盘服务，其中容量盘占比 85%；SSD 盘占比 15%。
可在脱机状态下在线挂载、卸载或扩展云硬盘。
云存储服务采用全冗余架构，无单点故障，服务可用性不低于 99.9%。
▲从主机端口到硬盘全路径支持基于硬件的并符合业界标准的 T10-PI 数据一致性检测，保障数据的一致性。
数据可销毁性：投标人承诺在用户要求删除数据或设备在弃置、转售前必须将其所有数据彻底删除，且无法复原。
▲数据可迁移性：投标人承诺用户能够控制数据的迁移，保证启用或弃用该云服务时，数据能迁入和迁出。
备份资源
备份资源要求和存储资源按 1:1 配置，支持基于硬件的并符合业界标准的 T10-PI 数据一致性检测，保障数据的一致性。
备份存储资源服务不少于 403T，具体要求如下。
▲支持基于硬件的并符合业界标准的 T10-PI 数据一致性检测，保障数据的一致性。

▲具备去零功能，提高空间利用率。
▲具备精简功能，实现存储空间超分配。
▲具备克隆功能。
▲具备在线重删压缩功能。
▲具备存储远程复制功能，至少必须包含异步复制。
互联互通专线
目前本地私有云与闵行区卫生网、公有云的互联互通是通过点对点专线连接到闵行区卫生网核心节点，既能满足互联访问的需要，也能够保障互联的安全。
本地私有云与闵行区卫生网互联专线的方案包括：两根 1000M 专线。
本地私有云与公有云互联专线的方案包括：二根 100M 专线。
专线的功能要求如下：
适用于任何高速率、信息量大、实时性强的业务传送；
带宽灵活，在 1M 到 10G 的区间内，可以灵活选择；
以太专线业务性能指标包括：吞吐量、时延、丢帧率。
吞吐量：指单位时间内成功地传送报文数量。测试值与承诺带宽误差应小于 1%。
时延：时延是指在两台 U 设备之间传送以太网帧所需的时间。上海境内平均时延≤10ms
丢帧率：指一定时间内以太网帧在 U 设备之间传送过程中丢掉的帧数占总发送帧数的百分比，平均丢帧率≤1×10-7
机房及配套

机房基本要求	
序号	要求
1	市电供应机房来自不同的局向。
2	通信网络来自不同的网络局端。
3	机房至少满足 60 个标准机柜，机柜配置为 19 英寸 42U 机柜。
4	周边范围应无剧烈爆炸源。
机房建筑要求	
序号	要求
5	机房大楼完善的防水防渗漏处理。
6	机房净高不低于 2.8 米。（高架地板到梁底或者吊顶）。
7	楼板承重不低于 6kN/ M2。
8	主机房不应布置在用水区域的垂直下方，不应与振动和电磁干扰源为邻。围护结构的材料选型应满足保温、隔热、防火、防潮、少灰尘等要求。 主机房应设置单独的出入口。 活动地板高度不应小于 300 毫米。 机房不应设有外窗，不应设置在地下室。
9	整个运输路径，所有通道、门、电梯宽度不小于 1.5 米，高度不小于 2.2 米，货梯载重能力不小于 2 吨。
市电输入要求	
序号	要求
10	两路来自不同局向的市电高压电专线供电。
11	自备 10KV 变电站两路市电间。

网络接入要求	
序号	要求
12	可以支持宽带资源。
13	网络机房内统一配备上走线桥架。
机房装修要求	
序号	要求
14	机房室内四周墙面气密性好、不易起尘、易清洁。
15	机房铺设架空活动防静电地板，地板以下净空不小于 30 厘米，地板均载承重不小于 6kN/ M2。
16	采用列间空调，单个微模块配置 4 台（3 用 1 备）显冷量约为 23kW 的风冷列间空调，正面送风背后回风。
17	机房内统一配备上走线桥架，供铜缆和光纤走线。
18	采用防静电地板敷设。
19	机柜布局应采用冷热通道分隔模式。
机房电力要求	
序号	要求
20	机柜插座为双路供电，每路配备 24 个 C13 插座。机柜插座必须从配电柜中各自独立的空气开关引出，提供的机柜电源必须是冗余的，1 路跳电不能影响另外 1 路。
21	按需提供单机柜电量 4KW。
22	配备 1 套 240V 直流系统，按通信负荷 240V/1000A 配置整流模块和蓄电池组，即蓄电池组满足负荷 240V/1000A 放电时间大于 15 分钟。
23	柴油发电机组为自启动，且市电电源与油机电源在低压配电系统中自动切换，市电正常时由市电供全楼的负荷用电，当一路市电失电时自动启动柴油发电机组供给保证负荷用电。
24	实现强弱电走线分离，均采用上走线方式。
25	配备双路市电、240V 高压直流系统和后备柴油发电机三重保障的高度冗余性的电力系统。
26	提供动力设施（如空调、照明、门禁等系统用电）的配电应独立于 IT 设备用电，必须从独立的配电柜引出。
27	机房接地系统和防雷系统性能良好，符合国家标准中的要求。
28	零地电压要求小于 1 伏特。
机房空调要求	
序号	要求
29	采用列间空调，单个微模块配置 4 台（3 用 1 备）显冷量约为 23kW 的风冷列间空调，正面送风背后回风。
	1)室内温度：23±1°C；
	2)相对湿度：40%-55%；
	3)温度变化率：<5°C/h 并不得结露。
30	机房精密空调需有一路市电、1 路油机供电。
综合布线要求	

序号	要求
31	铜缆布线：采用上走线方式。
32	光缆布线：采用上走线方式。
33	强电、弱电布线到机柜，可供 IT 设备直接使用。
34	铜缆和光纤的铺设到机柜。
机房监控要求	
序号	要求
35	安保监控：至少包括机房门禁独立管理、门禁状态监控、CCTV 摄像头实时监控系统，历史数据保存 3 个月。
36	机房动力监控：至少包括配电开关监控、配电参数监测（包括动力配电）。
37	机房环境监控：至少包括空调状态参数监控、温湿度监控、漏水检测、消防监控。
机房消防要求	
序号	要求
38	机房内须配备气体灭火系统，消防系统具备自动报警功能，须通过当地消防局验收。
机房安全及管理要求	
序号	要求
39	未经客户允许，任何其他公司的设备不能接入客户网络。
40	环境和设备监控系统应易于扩展和维护，并应具备显示、记录、控制、报警、分析和提示功能 机房设有独立的出入口控制系统，机房出入口设有专职安保人员
41	监控室应有 CCTV 摄像头监控界面、机房动力及环境监控。
服务要求	
序号	要求
42	中标供应商需提供 7*24 小时事件通知服务，通过 IT 服务管理工具、电话、短信、电子邮件等方式向采购人进行事件通告
43	供应商应为采购人免费办理长期园区及机房出入许可手续，便于采购人日常出入园区。
44	协助供应商建立应急处理机制，做好机房应急预案，在网络、电力、安全等各方面提供协助，确保采购人应急人员、设备和供应商能在最短时间内能够进入机房进行应急处置
45	供应商在进行重大变更时，应提前至少 10 天通过书面方式通知采购人，并告知确切影响以及应对预案
46	供应商应配备 7×24 小时值班保安人员，负责机房的安全保卫工作
47	供应商应日常机房巡检工作（包括机房环境、温湿度、安防、设备告警指示灯等、卫生状况）不少于每日 1 次，并留有记录，采购人有权调阅相关记录

密码服务

以密码技术为根本，以《网络安全等级保护基本要求》为目标，充分遵循《信息系统密码应用基本要求》的相关要求，建设面向云平台租户的密码服务体系，整体构建以密码技术为核心的云密码保障体系，融合密码应用的不同类别和多种场景，在保证安全合规的前提下，为云平台租户业务应用提供统一安全的密码服务。

4.2.6.1 密码服务依据：

(1)依法依规，紧扣需求

云密码保障体系应遵循《中华人民共和国网络安全法》和《网络安全等级保护条例》、《信息安全技术 网络安全等级保护基本要求》、《关键信息基础设施保护条例》、《信息系统密码应用基本要求》等相关政策法规和标准规范要求，以业务需求为导向，依法合规构建密码服务能力，确保业务系统密码应用的自主可控、安全可靠。

（2）技管并重，融合发展

先进成熟的密码应用体系是信息系统安全运行的必备前提，构建云密码保障体系的设备管理系统和密钥管理体系，实现技术体系建设和管理体系建设的有效融合，技术与管理双管齐下，融合发展，确保平台能够做到技术防护有效、管理保障到位的安全保障效果。

(3)统建共管，按需服务

通过规划和建设统一的密码基础设施和密码服务平台，为云平台租户中的应用系统提供符合自身安全需求的密码服务，避免重复建设。

(3)集约高效、开放融合。

加强统筹规划，实现密码与信息化基础设施、平台和应用的共建共享，降低建设运维成本，提高资金使用效益。有效整合资源，形成良好格局，推动信息化创新发展。

4.2.6.2 密码服务要求

要求密码服务系统可承载应用系统数据流量峰值不高于 1Gbps，应用系统加密访问人员不多于 300 用户（管理运维人员）的密码应用使用需求，可以实现数据传输加密与数据存储加密效果，符合密评工作相关要求。

具体密码服务内容清单：

安全层面	指标要求	系统密码应用需求	不适用说明
网络和通信安全	身份鉴别	确认通信实”的身份真实性，防止与假冒实”进行通信	无
	通信数据完整性	保护通信过程中重要数据的完整性和机密性，防止数据被非授权篡改，防止敏感数据 泄露	无
	通信数据机密性		
	网络边界访问控制信 息完整性	保护网络边界设备中的访问控制信息的完整性，防止被非授权篡改	无
	安全接入认证	对外部连接到内部网络的设备进行接入认证，确保接入设备身份真实性	无
设备和计算安全	身份鉴别	对系统管理员的身份真实性进行识别和确认，防止假冒人员登录	无
	安全的信息传输通道	建立系统安全的数据传输通道	无
	重要信息资源安全标记完整性	不适用	无重要信息资源敏感标记的情况
	访问控制信息完整性	保护计算机、服务器等设备中的系统资源访问控制信息、日志记录和重要可执行程序的完整性，防止被非授权篡改，确保重要可执 行程序来源真实性	无
	日志记录完整性		无
	重要可执行程序完整性、重要可执行程序 来源真实性		无
应用和数据安全	身份鉴别	确认 PC 端登录用户的身份真实 性，防止假冒人员登录	无

访问控制信息完整性	对访问权限控制列表进行完整性保护，防止被非授权篡改	无
重要数据传输机密性 重要数据存储机密性 重要数据传输完整性 重要数据存储完整性	保护在客户端与服务器之间、应用系统之间的非安全网络信道中传输的和存储的用户登录身份鉴别信息、医卫云信息数据的机密性 和完整性，防止数据泄露给非授权的个人、进程等	无
重要信息资源安全标记完整性	不适用	无重要信息资源敏感标记情况
不可否认性	在涉及法律责任认定的应用中，用密码技术保护数据原发证据和接受证据的不可否认性	无

4.2.6.3 密码安全要求

根据《基本要求》中安全管理制度方面的要求，制定与本次项目 涉及的信息系统相适应的密码安全管理制度和操作规范，内容包含密 码建设、运维、人员、设备、密钥等 6 个方面。

根据《基本要求》中安全管理人员方面的要求，对本次项目涉及的信息系统现有的人员管理制度进行补充和完善，要求设置内部密码专题培训机制，每 3 个月组织一次，由应标人员或聘请外部专家担任培训讲师，内容涉及密码相关法律法规和标准 规范、商用密码应用、商用密码应用安全性评估等多个方面，使相关人员了解密码相关的法律和法规，掌握密码基本原理，并遵照执行。

根据《基本要求》中安全管理应急方面的要求，对本次项目涉及的信息系统现有的应急管理制度进行完善，补充制定密码相关应急处置预案，并做好应急资源准备，明确密码安全事件处理流程及其它管理措施。

4.2.6.4 密码服务具体产品及性能要求

产品清单：

产品型号	数量
信安应用安全网关系统 V8.0NSAE1800	2
信安 CCypher 云密码服务平台 V2.7 CCypher8000	2
信安签名验签系统 vNetSign 8G V2.7vNetSign 8G	2
信安动态密码系统 vNetPas 8G	2
信安数据加解密服务系统 vNetEDS	1
信安密钥管理系统 SYT1902	1

性能要求：

安全认证网关 信安应用安全网关系统 V8.0 NSAE1800	
功能项	功能及技术参数
硬件要求	标准 1U 设备，支持双电源，不少于 2 核 4 线程 CPU X1，不少于 1T 硬盘，不少于 8G 内存，不少于 4 个千兆电口。设备面板要求具有告警灯、电源提示灯、运行指示灯；
	必须使用专用系统，不得使用基于 Linux 或 Windows 的操作平台，且承诺无公开安全漏洞。
	支持 SSL 多卡硬件加速

设备性能	SSL 吞吐率(SM2)不少于 750Mbps SSL 每秒新建连接数(SM2)不少于 3.5K TPS SSL 最大并发连接数(SM2)不少于 220K TPS SSL 吞吐率(RSA2048)不少于 3.00Gbps SSL 每秒新建连接数(RSA2048)不少于 2.2K TPS SSL 最大并发连接数(RSA2048)不少于 500K TPS （SSL 均为单向认证性能） 四层吞吐率不少于 7.60Gbps 四层每秒新建连接数不少于 420K CPS 四层最大并发连接数不少于 8M 七层吞吐率不少于 7.40Gbps 七层每秒请求数不少于 1M RPS 七层最大并发连接数不少于 1.2M （七层性能为连接复用模式）
算法支持	对称算法：SM4、DES、AES 等 非对称算法：SM2、RSA 等 摘要算法：SM3、SHA-1、SHA256、MD5 等
功能要求	支持证书字段透传功能，转发模式包括 URL、cookie、header 且可自定义名称；
	支持识别数字证书同步报文和业务 API 加签报文， 能够指定域内签名签名服务器进行验签名；（要求提供产品截图证明材料，并加盖原厂商公章）
	支持 SSL 拦截白名单，只允许通过指定的域名访问特定的 SSL 服务；
	支持透明模式、反向代理模式以及三角传输模式，支持旁路连接方式（单臂模式）和串连连接方式（双臂模式）。
	支持多种高可用性模式：A/A 模式，A/S 模式，支持多台设备的集群，支持双机 failover 切换功能，能够及时发现设备故障，支持会话同步；
	支持通过 WEBUI、CLI 进行完整配置以及设备管理；
	可支持服务器负载均衡功能，负载均衡算法提供最少连接数、轮询、最快响应时间、最小带宽使用率等负载均衡算法，支持 20 种以上负载均衡算法。（要求提供产品截图证明材料，并加盖原厂商公章）
	支持丰富的健康检查方法，包括但不限于：ICMP、TCP、UDP、HTTP、HTTPS、FTP、SNMP、DNS 等多种服务器健康检查方式，且设备能够支持通过 SCRIPT-TCP、SCRIPT-UDP 应用脚本方式，对服务器的 FTP, SMTP, LDAP, RADIUS, POP3, DNS, TELNET 等多种应用进行检查（要求提供产品截图证明材料，并加盖原厂商公章）
	支持高可靠性 HA，支持以 CPU 温度、CPU 使用率、SSL 加速卡等作为阈值监控对象，并支持基于“与”、“或”等逻辑关系运算组合监控对象进行 HA 切换，并且 HA 设备之间能够实现配置同步和会话状态同步。(提供功能截图证明，并加盖原厂商公章）
	支持客户端证书过滤功能，支持基于 issus、subject 等项拒绝连接；（要求提供产品截图证明材料，并加盖原厂商公章）
资质要求	具备国家密码管理局所颁发的《商用密码产品认证证书》
	提供 ssl 以及数字签名功能的客户端作为配套，客户端具备对应产品型号证书
	具备公安部所颁发的《《计算机信息系统安全专用产品销售许可证》且产品类型为“访问控制（网络-基本级）
	具备全球 IPv6 测试中心颁发的《IPv6 Logo 认证证书》
	具备保密局颁发的《涉密信息系统产品检测证书》
	同系列产品具备两家以上第三方检测中心（赛宝实验室、质量认证中心、公安部信息安全产品检测中心）出具的检测报告（要求提供检测报告关键页）

全密码服务平台 信安 CCypher 云密码服务平台 V2.7 CCypher8000	
指标项	功能及技术参数
硬件要求	标准 1U 或 2U 设备，支持双电源，不少于 4 核 8 线程 CPU X1，不少于 2T 硬盘，不少于 64G 内存，不少于 8 个千兆电口
性能要求	四层每秒新建连接数不少于 1.12M CPS 四层最大并发连接数不少于 8M 四层吞吐率不少于 38.15Gbps 七层每秒新建连接数不少于 266K RPS 七层最大并发连接数不少于 1.2M 七层吞吐率不少于 26.35Gbps；
系统管理	需支持管理员访问权限控制
	需支持 WebUI 和 CLI 命令行配置
	需支持管理接口配置 IP 地址
	需支持 XML-RPC 接入
	需支持 RESTful API 接入
设备虚拟化能力	设备需支持密码服务虚拟化功能，支持通过镜像模板快速创建虚拟机，支持通过向虚拟机导入镜像模板的方式快速创建密码服务
	虚拟机需支持静态聚合和动态聚合
	虚拟机需支持独享硬件资源，包括 CPU、内存、网卡、SSL 卡等，保证各网络功能或安全功能之间的资源不争抢，确保单一密码服务具有性能保障。（要求提供产品截图证明材料，并加盖原厂商公章）
	需支持密码计算卡虚拟化，各虚拟化实例完全独立，互不影响
虚拟交换机	产品需支持虚拟交换机功能
	产品需支持通过虚拟交换机配置 VLAN 或 VXLAN 技术将各虚拟密码服务实例进行安全隔离。（要求提供产品截图证明材料，并加盖原厂商公章）
	虚拟交换机需支持 STP。（要求提供产品截图证明材料，并加盖原厂商公章）
	需支持端口镜像。（要求提供产品截图证明材料，并加盖原厂商公章）
	需支持原生模式和调优模式。（要求提供产品截图证明材料，并加盖原厂商公章）
虚拟化实例管理	产品需支持部署数字证书认证系统服务实例
	产品需支持部署签名验签服务实例，并能监控服务实例运行状态。（要求提供产品截图证明材料，并加盖原厂商公章）
	产品需支持部署动态密码服务实例，并能监控服务实例运行状态。（要求提供产品截图证明材料，并加盖原厂商公章）
	产品需支持部署数据加解密服务实例，并能监控服务实例运行状态。（要求提供产品截图证明材料，并加盖原厂商公章）
	产品需支持密码实例之间配置隔离、故障隔离、性能隔离
	产品需支持对各密码服务实例进行集中管理。（要求提供产品截图证明材料，并加盖原厂商公章）
	需支持使用预定义和自定义资源分配模板创建虚拟机
	需支持调整虚拟机资源分配
	需支持多级别的高可用性，为平台和承载的功能实例提供冗余和失效切换。承载的功能实例可以进行失效切换，也可以在主备平台间切换
高可用性	需支持主/备、主/主模式

（HA）	需支持同步功能
	需支持 HA 告警功能，当主/备机 up 或者 down 时，允许系统给管理员发送告警邮件
问题解决工具	需支持 ping、ping6、traceroute、traceroute6
	需支持收集调试数据
运维管理功能	需支持统一配置运维管理功能，支持对各虚拟密码服务进行集中创建、启动、停止、删除等管理工作；支持对各密码服务集中配置管理、服务状态监控、集中运维管理等工作。
集成管理能力	产品需支持通过 eCloud API、RESTful API 等接口提供与云平台管理、编排和自动化系统集成的能力，支持实现对设备和密码服务的管理和监控
产品资质	产品需具备国家密码管理局颁发的《商用密码产品认证证书》。

签名验签系统 信安签名验签系统 vNetSign 8G	
功能项	功能及技术参数
性能要求	签名：RSA2048：1000TPS，SM2：20KTPS； 验签：RSA2048：22000TPS，SM2：15KTPS
算法支持	对称算法：DES、3DES、AES、SM4 等 非对称算法：RSA、SM2 等 摘要算法：SHA-1、SHA256、HMAC、SM3 等
功能要求	单台设备支持配置多个签名验签服务
	支持 Attached 签名验签、Detached 签名验签、attached 事后验签、RAW 签名验签、XML 封皮签名验签、XML 封内签名验签、XML 分离签名验签；
	支持提供数字信封功能对原文数据高强度加解密、支持 HMAC 加解密；
	支持基于 IP 地址校验和基于访问口令校验的安全访问，只允许合法的业务应用通过 API 访问，防止恶意访问。（要求提供产品截图证明材料，并加盖原厂商公章）
	支持设备监控包括可监控 CPU 温度、风扇转速、CPU 使用率、网口流量等状态。（要求提供产品截图证明材料，并加盖原厂商公章）
	支持弱算法过滤，可灵活配置摘要算法是否允许签名和验签名、非对称算法的秘钥长度、对称算法是否允许加密或解密；(提供投标产品功能截图，并加盖原厂商公章)；
	支持对 PDF 文件格式进行电子签名和验证，可自定义签名区域内显示的图章、说明文字及签名证书信息。
	要求设备支持提供 SDF 接口，具备非对称、对称及杂凑运算和密钥管理 SDF 接口。
	支持生产系统和灾备系统之间远程证书同步、支持 3 套系统以上之间机构证书同步，（提供产品截图并加盖原厂商公章）。
资质要求	具备国家密码管理局商用密码检测中心颁发的《商用密码产品认证证书》
	具备公安部所颁发的《计算机信息系统安全专用产品销售许可证》且产品类型为“不可否认性鉴别”
	具备国家版权局颁发的《计算机软件著作权登记证书》

动态密码系统 信安动态密码系统 vNetPas 8G	
功能项	功能及技术参数
性能要求	包含 300 用户授权（管理运维人员） 响应性能 500TP

算法支持	对称算法：SM4 非对称算法：SM2 摘要算法：SM3
功能要求	包含管理模块、生成模块、验证模块；支持三个模块独立运行，独立管理；支持单独模块的负载均衡。（提供产品功能截图证明材料，并加盖原厂商公章）
	支持硬件令牌、手机令牌、手机短信等多种形态的动态密码。需提供独立的 agent 客户端，兼容国产操作系统，实现系统用户通过一次性验证口令登录操作系统。
	提供移动端 APP 令牌，支持 android 和 IOS 移动端 OS。APP 支持与移动管理平台无缝对接，生成基于国密算法产生一次性验证密码。 手机令牌 APP 支持通过数字证书方式进行验证、存储动态口令种子，支持数字签名、验证等密码操作。
	提供完善的动态密码管理功能，包括启用、挂失、解除挂失、停用、锁定、替换、查询等功能。当动态令牌被锁定时，管理员可以通过管理功能解锁。满足国内通用双因素认证机制及 TOP（一次一密）、SM3 国密算法，加密密钥确保唯一性，且长度不小于 160 位，且支持挑战应答模式。
	提供详细的统计功能，能够对多品牌、多渠道、不同状态下的动态令牌进行分类统计，并生成报表导出。具有丰富的审计功能。审计管理支持查询业务日志功能，应提供丰富的查询条件与简单易用的查询界面，支持多条件复合查询，查询结果支持按业务操作时间排序；审计管理支持查询系统日志，具体包括系统运行日志、系统管理日志、帐户日志等，对于事件来源和产生者还应提供详细记录，提供多种灵活的报表统计形式。
	支持无线接入时，通过 RADIUS PEAP、PAP、CHAP、MSCHAP/MSCHAPV2 协议认证接入。
	支持 LDAP 数据同步功能，支持 SSL 加密传输。（提供产品功能截图证明材料，并加盖原厂商公章）
	支持种子生成双人审核机制。（提供产品功能截图证明材料，并加盖原厂商公章）
	支持生成加密的动态口令。
	要求配套客户端软件支持安卓、IOS、H5 等多种形式，要求客户端 APP 能够在安卓、IOS 应用市场直接下载使用。
	支持对口令验证、验证服务器连接数、验证服务器活动连接数、数据库连接池大小、数据库链接剩余大小等指标进行监控统计。（提供产品功能截图证明材料，并加盖原厂商公章）
	提供配套的客户端控件，支持通过动态口令方式登录操作系统（windows、linux 等）（提供产品功能截图证明材料，并加盖原厂商公章）
	支持 Windows 系统同一系统账号映射不同用户名，使用用户名进行系统登录时可以从日志从查看实际登录的账号与用户名（提供产品功能截图证明材料，并加盖原厂商公章）
资质要求	要求提供国家密码管理局颁发的《商用密码产品认证证书》
	要求提供公安部颁发的《计算机信息系统安全专用产品销售许可证》
	要求提供中华人民共和国国家版权局颁发的《计算机软件著作权登记证书》
	要求提供公安部信息安全产品检测中心出具的《检验检测报告》
	要求提供移动端动态令牌软件的《计算机软件著作权登记证书》

存储加密系统 信安数据加解密服务系统 vNetEDS	
功能项	功能及技术参数
性能要求	最大在线加解密吞吐量（SM4）：1Gbps 最大每秒在线加解密处理能力（SM4）：5000
算法支持	对称算法：SM4 非对称算法：SM2 摘要算法：SM3

协议支持要求	要求支持 GM/T 0110-2021《密钥管理互操作协议规范》、GB/T 38636-2020《信息安全技术传输层密码协议(TLCP)》协议；
通用加解密功能	要求支持对称密钥和非对称密钥加解密、支持签名验签、生成随机数、生成数字信封、生成摘要；支持提供 SDK，支持在线加密和本地加密两种加密方式；
	系统对外提供 RESTful 形式接口，接入应用通过授权应用 id 和授权密钥、token 等信息，完成接口调用的安全认证。
认证与访问控制要求	支持国密数字证书的 USBkey 方式登录系统，满足密码测评要求。（要求提供产品截图证明材料，并加盖原厂商公章）；
	支持三权分立，支持安全管理员角色、系统管理员角色、审计员角色，不同角色具有不同的权限。
	支持基于属性的访问控制（ABAC），支持应用密钥操作权限管理、应用 IP 白名单管理以及资源管理；
系统功能要求	支持系统数据的备份与恢复功能，支持系统跨版本升级和恢复
	支持服务管理：新增、启停、服务类型（通用加密、KMIP、切面加密）、SSL 证书；
	支持独立的多服务管理，可自定义服务类型、服务端口、加密策略
	支持一键巡检：对网络、加密卡、HA、SSL、密码算法等关键系统功能进行检查，并输出结果（要求提供产品截图证明材料，并加盖原厂商公章）；
	支持 SSL 配置：可开关 SSL，可配置 SSL 端口和站点证书。支持以 https 协议进行 Web 管理；
	支持 web 管理平台按时间维度统计密钥数量、新增趋势、使用量、使用排行、展示 CPU、内存、磁盘、网络的使用情况、展示版权、产品型号和 License 信息。（要求提供产品截图证明材料，并加盖原厂商公章）
	支持日志审计功能，通过 HMAC 保护系统日志的完整性。（要求提供产品截图证明材料，并加盖原厂商公章）
	支持敏感数据脱敏，并支持自定义脱敏策略；（要求提供产品截图证明材料，并加盖原厂商公章）
	支持数据库切面加解密配置管理、策略管理，支持保留格式加密，数据格式长度不变；（要求提供产品截图证明材料，并加盖原厂商公章）
资质要求	要求提供国家密码管理局所颁发的《商用密码型号认证证书》

密钥管理系统 信安密钥管理系统 SYT1902	
功能项	功能及技术参数
性能要求	密钥容量不少于 10000 张
算法支持	对称算法：SM4 非对称算法：SM2 摘要算法：SM3
密钥管理要求	支持对称密钥和非对称密钥的生成、更新、备份、恢复、归档、销毁等安全生命周期管理操作；支持以密钥分量方式导入/导出根密钥，支持以密码信封方式导入/导出对称和非对称密钥，支持多种门限方案的密钥备份与恢复机制，并且支持密钥跨版本恢复
	支持密钥轮转机制，并可自定义轮转周期
	支持密钥别名管理
	支持设置密钥计划删除周期，并可对系统中近三天内即将被删除的密钥进行告警提示
	支持与公有云密钥管理系统对接，实现公有云基础设备密钥管理
KMIP 加密功能要求	支持 KMIP1.4 及国密标准密钥管理互操作协议的对称密钥和非对称密钥加解密
	支持 KMIP1.4 及国密标准密钥管理互操作协议的签名验签、杂凑、获取随机数、MAC 以及 MAC 验证
	支持 KMIP 密钥的全生命周期管理：预激活、激活、停用、失信、销毁、失信销毁等

	支持设置密钥用途掩码功能
	支持设置租约和使用限额
	支持 KMIP 客户端管理：支持新增、删除、停用 KIMP 客户端，可配置 KMIP 客户端认证方式、通信方式、操作权限等
	支持 XML、JSON、TTLV 编码格式
系统管理要求	支持国密 SSL 实现安全通信
	支持 web 管理平台按时间维度统计密钥数量、新增趋势、使用量、使用排行，展示 CPU、内存、磁盘、网络等的使用情况
	支持系统告警，包括：计划删除的密钥告警、在用库上限告警、开始 HA 后异常报警等
	支持双机主备、集群等部署方式，支持 HA 配置，实现 SSL、DB、密钥、服务配置等自动同步
资质要求	要求提供国家密码管理局所颁发的《商用密码型号认证证书》

4.2.6.5 密码服务运维要求

产品安装服务：产品安装服务包括现场安装和远程安装支持，需协助用户完成产品部署，部署完成后形成实施手册并提交。

定期巡检服务：供应商需每季度对密码设备进行巡检，巡检内容包括但不限于：设备硬件运行状态巡检、存储使用情况、数据连续性等，巡检完成后提交设备巡检报告。

远程技术支持服务：提供客户服务热线，为密码产品的突发故障问题提供远程技术支持，远程协助问题处理，快速处置，减少因故障带来的影响。

应急响应服务：当软件出现重大故障，远程支持无法解决问题时，由供应商安排工程师进行现场问题排查，工程师需在故障发生 2 小时内抵达现场并开展应急工作。应急工作完成后提交应急报告。

培训服务：针对安全运维管理人员进行理论和实际操作的培训，以帮助参培人员利用密码设备在实际工作中最大的发挥作用。

安全

闵行区医卫云由于自身对安全的高要求，因此需要平台将内网及卫生网应用、互联网应用、电子政务外网应用部署在不同的资源池，通过安全隔离、安全策略、灾备等来保证业务的安全性、便利性和可服务性。

本项目需开展重要信息系统等保测评、定级备案工作。要求私有云机房符合等保 2.0 三级，同时医卫云云平台通过三级等保测评，并协助甲方进行应用软件等保测评。测评过程发现的问题若属于私有云范围，投标人进行整改。本项目的安全要求符合以下建设依据和标准。

项目的建设要满足以下建设依据和标准：

《政务信息资源交换体系》GB/T21062；

《信息安全技术信息系统安全等级保护基本要求》（GB/T 22239-2008）；

《中华人民共和国计算机信息系统安全保护条例》国务院令 147 号 1994 年 2 月 18 日；

《电子计算机机房设计规范》（GB50174-93）；

国家发布的相关政策及法规等。

▲私有云平台要符合等保 2.0 三级的要求，需要从安全物理环境、安全通信网络、安全区域边界、安全计算环境、安全管理中心、安全管理制度、安全管理机构、安全管理人员、安全建设管理、安全运维管理方面提供安全服务，从而满足平台网络安全、系统安全、数据安全等的安全需要。平台上的业务系统、所有数据的拥有权及使用权均属于采购方，中标人无权对其进行支配，所有设备的使用、关闭、维修、报废等处理需经云平台管理单位同意，并在监管下进行。若发现中标人未经许可对业务系统和数据进行支配，采购人将对中标人采取惩罚措施并追究其法律责任。

安全物理环境

平台要提供安全物理环境设计，参考以下内容，达到等保 2.0 三级评测功能要求：

物理位置，机房场地要求选择在具有防震、防风和防雨等能力的建筑内。机房场地要求避免设在建筑物的顶层或地下室，否则要求加强防水和防潮措施。要求保证云计算基础设施位于中国境内。

访问控制，机房出入口要求配置电子门禁系统，控制、鉴别和记录进入的人员。

安全通信网络

平台要提供安全通信网络设计，参考以下内容，达到等保 2.0 三级评测功能要求：

▲公有云、卫生网等接入网路的安全要求通过防火墙进行隔离和防护，将外网访问的流量制定严格精细的安

全策略，对数据包进行状态化的实时监测，将可信的访问进行放行，对不符合安全规则的访问进行阻断。
网络架构，要求保证网络设备的业务处理能力满足业务高峰期需要。要求保证网络各个部分的带宽满足业务高峰期需要。要求划分不同的网络区域，并按照方便管理和控制的原则为各网络区域分配地址。要求避免将重要网络区域部署在边界处，重要网络区域与其他网络区域之间要求采取可靠的技术隔离手段。要求提供通信线路、关键网络设备和关键计算设备的硬件冗余，保证系统的可用性。要求保证云计算平台不承载高于其安全保护等级的业务要求用系统。要求实现不同云服务用户虚拟网络之间的隔离。要求具有根据云服务用户业务需求提供通信传输、边界防护、入侵防范等安全机制的能力。要求具有根据云服务用户业务需求自主设置安全策略的能力，包括定义访问路径、选择安全组件、配置安全策略。要求提供开放接口或开放性安全服务，允许云服务用户接入第三方安全产品或在云计算平台选择第三方安全服务。
通信传输，要求采用校验技术或密码技术保证通信过程中数据的完整性。要求采用密码技术保证通信过程中数据的保密性。云平台的通信安全应部署 VPN 系统，以便提供给远程访问云服务的用户安全连接，并建立双向的身份验证机制。
可信验证，可基于可信根对通信设备的系统引导程序、系统程序、重要配置参数和通信要求用程序等进行可信验证，并在要求用程序的关键执行环节进行动态可信验证，在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。
安全区域边界
平台要提供安全区域边界设计，参考以下内容，达到等保 2.0 三级评测功能要求：
边界防护，要求保证跨越边界的访问和数据流通过边界设备提供的受控接口进行通信。要求能够对非授权设备私自联到内部网络的行为进行检查或限制。要求能够对内部用户非授权联到外部网络的行为进行检查或限制。要求限制无线网络的使用，保证无线网络通过受控的边界设备接入内部网络。
访问控制，要求在网络边界或区域之间根据访问控制策略设置访问控制规则，默认情况下除允许通信外受控接口拒绝所有通信。要求删除多余或无效的访问控制规则，优化访问控制列表，并保证访问控制规则数量最小化。要求对源地址、目的地址、源端口、目的端口和协议等进行检查，以允许/拒绝数据包进出。要求能根据会话状态信息为进出数据流提供明显的允许/拒绝访问的能力。要求对进出网络的数据流实现基于要求用协议和要求用内容的访问控制。要求在虚拟化网络边界部署访问控制机制，并设置访问控制规则。要求在不同等级的网络区域边界部署访问控制机制，设置访问控制规则。
入侵防范，要求在关键网络节点处检测、防止或限制从外部发起的网络攻击行为。要求在关键网络节点处检测、防止或限制从内部发起的网络攻击行为。要求采取技术措施对网络行为进行分析，实现对网络攻击特别是新型网络攻击行为的分析。当检测到攻击行为时，记录攻击源 IP、攻击类型、攻击目标、攻击时间，在发生严重入侵事件时要求提供报警。要求能检测到云服务用户发起的网络攻击行为，并能记录攻击类型、攻击时间、攻击流量等。要求能检测到对虚拟网络节点的网络攻击行为，并能记录攻击类型、攻击时间、攻击流量等。要求能检测到虚拟机与宿主机、虚拟机与虚拟机之间的异常流最。要求在检测到网络攻击行为、异常流量情况时进行告警。
防范恶意代码和垃圾邮件，要求在关键网络节点处对恶意代码进行检测和清除，并维护恶意代码防护机制的升级和更新。要求在关键网络节点处对垃圾邮件进行检测和清除，并维护垃圾邮件防护机制的升级和更新。
可信验证，可基于可信根对边界设备的系统引导程序、系统程序、重要配置参数和边界防护要求用程序等进行可信验证，并在要求用程序的关键执行环节进行动态可信验证，在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。
防病毒：在关键网络节点部署专用网络防病毒系统（设备），提供病毒防护能力，通过对恶意代码进行检测和清除，并维护恶意代码防护机制的升级和更新，有效限制病毒随互联网访问、远程运维途径进入到云平台当中，同时能防止病毒在云平台内传播扩散，同时提供和安装各服务器病毒查杀软件，定期查杀，定期病毒库升级等。
安全计算环境
平台要提供安全计算环境设计，参考以下内容，达到等保 2.0 三级评测功能要求：
身份鉴别，要求对登录的用户进行身份标识和鉴别，身份标识具有唯一性，身份鉴别信息具有复杂度要求并定期更换。要求具有登录失败处理功能，要求配置并启用结束会话、限制非法登录次数和当登录连接超时自动退出等相关措施。当进行远程管理时，要求采取必要措施防止鉴别信息在网络传输过程中被窃听。要求采用口令、密码技术、生物技术等两种或两种以上组合的鉴别技术对用户进行身份鉴别，且其中一种鉴别技术至少要求使用密码技术来实现。当远程管理云计算平台中设备时，管理终端和云计算平台之间要求建立双向身份验证机制。

访问控制，要求对登录的用户分配账户和权限。要求重命名或删除默认账户，修改默认账户的默认口令。要求及时删除或停用多余的、过期的账户，避免共享账户的存在。要求授予管理用户所需的最小权限，实现管理用户的权限分离。要求由授权主体配置访问控制策略，访问控制策略规定主体对客体的访问规则。访问控制的粒度要求达到主体为用户级或进程级，客体为文件、数据库表级。要求对重要主体和客体设置安全标记，并控制主体对有安全标记信息资源的访问。要求保证当虚拟机迁移时，访问控制策略随其迁移。要求允许云服务用户设置不同虚拟机之间的访问控制策略。
入侵防范，要求遵循最小安装的原则，仅安装需要的组件和要求用程序。要求关闭不需要的系统服务、默认共享和高危端口。要求通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制。要求提供数据有效性检验功能，保证通过人机接口输入或通过通信接口输入的内容符合系统设定要求。要求能发现可能存在的已知浦洞，并在经过充分测试评估后，及时修补漏洞。要求能够检测到对重要节点进行入侵的行为，并在发生严重入侵事件时提供报警。要求能检测虚拟机之间的资源隔离失效，并进行告警。要求能检测非授权新建虚拟机或者重新启用虚拟机，并进行告警。要求能够检测恶意代码感染及在虚拟机间蔓延的情况，并进行告警。
恶意代码防范，要求采用免受恶意代码攻击的技术措施或主动免疫可信验证机制及时识别入侵和病毒行为，并将其有效阻断。
可信验证，可基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和要求用程序等进行可信验证，并在要求用程序的关键执行环节进行动态可信验证，在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。
镜像和快照保护，要求针对重要业务系统提供加固的操作系统镜像或操作系统安全加固服务。要求提供虚拟机镜像、快照完整性校验功能，防止虚拟机镜像被恶意篡改。要求采取密码技术或其他技术手段防止虚拟机镜像、快照中可能存在的敏感资源被非法访问。
数据完整性和保密性，要求采用校验技术或密码技术保证重要数据在传输过程中的完整性，包括但不限于鉴别数据、重要业务数据、重要审计数据、重要配置数据、重要视频数据和重要个人信息等。要求采用校验技术或密码技术保证重要数据在存储过程中的完整性，包括但不限于鉴别数据、重要业务数据、重要审计数据、重要配置数据、重要视频数据和重要个人信息等。要求采用密码技术保证重要数据在传输过程中的保密性，包括但不限于鉴别数据、重要业务数据和重要个人信息等。要求采用密码技术保证重要数据在存储过程中的保密性，包括但不限于鉴别数据、重要业务数据和重要个人信息等。要求确保云服务用户数据、用户个人信息等存储于中国境内，如需出境要求遵循国家相关规定。要求确保只有在云服务用户授权下，云服务商或第三方才具有云服务用户数据的管理权限；要求使用校验码或密码技术确保虚拟机迁移过程中重要数据的完整性，并在检测到完整性受到破坏时采取必要的恢复措施。要求支持云服务用户部署密钥管理解决方案，保证云服务用户自行实现数据的加解密过程。
数据备份恢复，要求提供重要数据的本地数据备份与恢复功能。利用通信网络将重要数据实时备份至备份场地。要求提供重要数据处理系统的热冗余，保证系统的高可用性。云服务用户要求在本地保存其业务数据的备份。要求提供查询云服务用户数据及备份存储位置的能力。云服务商的云存储服务要求保证云服务用户数据存在若干个可用的副本，各副本之间的内容要求保持一致。要求为云服务用户将业务系统及数据迁移到其他云计算平台和本地系统提供技术手段，并协助完成迁移过程。
剩余信息保护，要求保证鉴别信息所在的存储空间被释放或重新分配前得到完全清除。要求保证存有敏感数据的存储空间被释放或重新分配前得到完全清除。要求保证虚拟机所使用的内存和存储空间回收时得到完全清除。云服务用户删除业务要求用数据时，云计算平台要求将云存储中所有副本删除。
个人信息保护，要求仅采集和保存业务必需的用户个人信息。要求禁止未授权访问和非法使用用户个人信息。
安全管理中心
平台要提供安全管理中心设计，参考以下内容，达到等保 2.0 三级评测功能要求：
系统管理，要求对系统管理员进行身份鉴别，只允许其通过特定的命令或操作界面进行系统管理操作，并对这些操作进行审计；要求通过系统管理员对系统的资源和运行进行配置、控制和管理，包括用户身份、系统资源配置、系统加载和启动、系统运行的异常处理、数据和设备的备份与恢复等。
安全管理，要求对安全管理员进行身份鉴别，只允许其通过特定的命令或操作界面进行安全管理操作，并对这些操作进行审计；要求通过安全管理员对系统中的安全策略进行配置，包括安全参数的设置，主体、客体进行统一安全标记，对主体进行授权，配置可信验证策略等。
集中管控，要求划分出特定的管理区域，对分布在网络中的安全设备或安全组件进行管控；要求能够建立一条安全的信息传输路径，对网络中的安全设备或安全组件进行管理；要求对网络链路、安全设备、网络设备

和服务器等的运行状况进行集中监测；要求对分散在各个设备上的审计数据进行收集汇总和集中分析，并保证审计记录的留存时间符合法律法规要求；要求对安全策略、恶意代码、补丁升级等安全相关事项进行集中管理；要求能对网络中发生的各类安全事件进行识别、报警和分析。
集中管控，要求能对物理资源和虚拟资源按照策略做统一管理调度与分配；要求保证云计算平台管理流量与云服务用户业务流量分离；要求根据云服务商和云服务用户的职责划分，收集各自控制部分的审计数据并实现各自的集中审计；要求根据云服务商和云服务用户的职责划分，实现各自控制部分，包括虚拟化网络、虚拟机、虚拟化安全设备等的运行状况的集中监测。
安全管理制度
平台要提供安全管理体系设计，参考以下内容，达到等保 2.0 三级评测功能要求：
平台要提供安全管理体系，通过制定完善、完整的安全管理制度，实现有目标、有方法、有记录的安全管理，具体包括以下四层：
第一层：安全策略，制定网络安全工作的总体方针和安全策略，阐明机构安全工作的总体目标、范围、原则和安全框架等。
第二层：管理制度，对安全管理活动中的各类管理内容建立安全管理制度；管理人员或操作人员执行的日常管理操作建立操作规程。
第三层：制定和发布，指定或授权专门的部门或人员负责安全管理制度的制定；安全管理制度要求通过正式、有效的方式发布，并进行版本控制。
第四层：评审和修订，定期对安全管理制度的合理性和适用性进行论证和审定，对存在不足或需要改进的安全管理制度进行修订。
安全管理机构
平台要提供安全管理机构设计，参考以下内容，达到等保 2.0 三级评测功能要求：
根据基本要求设置安全管理机构的组织形式和运作方式，明确岗位职责；
设置安全管理岗位，设立系统管理员、审计管理员、安全管理员等岗位，根据要求进行人员配备，配备专职安全员；成立指导和管理信息安全工作的委员会或领导小组，其最高领导由单位主管领导担任或授权；制定文件明确安全管理机构各个部门和岗位的职责、分工和技能要求。
建立授权与审批制度；
建立内外部沟通合作渠道；
定期进行全面安全检查，特别是系统日常运行、系统漏洞和数据备份等。
安全管理人员
平台要提供安全管理人员设计，参考以下内容，达到等保 2.0 三级评测功能要求：
根据基本要求制定人员录用、离岗、安全意识教育和培训几个方面的规定，并严格执行；规定外部人员访问流程，并严格执行。
安全建设管理
平台要提供安全建设管理设计，参考以下内容，达到等保 2.0 三级评测功能要求：
根据基本要求制定系统建设管理制度，包括：系统定级备案、安全方案设计、产品采购和使用、自行软件开发、外包软件开发、工程实施、测试验收、系统交付、等级评测、服务供应商选择等方面。从工程实施的前、中、后三个方面，从初始定级设计到验收评测完整的工程周期角度进行系统建设管理。
云服务商其所提供的云平台应为其所承载的业务应用系统提供相应等级的安全保护能力；应在服务水平协议中规定云服务的各项服务内容和具体技术指标；应在服务水平协议中规定云服务商的权限与责任，包括管理范围、职责划分、访问授权、隐私保护、行为准则、违约责任等；应在服务水平协议中规定服务合约到期时，完整地返还云服务客户信息，并承诺相关信息在云计算平台上清除；应与选定的云服务商签署保密协议，要求其不得泄露云服务客户数据和业务系统的相关重要信息；应确保供应商的选择符合国家有关规定；应将供应链安全事件信息或威胁信息及时传达到云服务客户；应将供应商的重要变更及时传达到云服务客户，并评估变更带来的安全风险，采取有关措施对风险进行控制。
安全运维管理
平台要提供安全运维管理设计，参考以下内容，达到等保 2.0 三级评测功能要求：
根据基本要求进行信息系统日常运行维护管理，利用管理制度以及安全管理中心进行，包括：环境管理、资产管理、介质管理、设备管理、监控管理和安全管理中心、网络安全管理、系统安全管理、恶意代码防范管理、密码管理、变更管理、备份与恢复管理、安全事件处置、应急预案管理等，使系统始终处于相应等级安全状态中。

云计算平台的运维地点应位于中国境内，境外对境内云计算平台实施运维操作应遵循国家相关规定。
私有云云管理平台
医卫云平台通过自动化的运维管理，提升用户 IT 人员的运维管理效率。基于资源池的统一编排和调度，实现对虚拟化环境和物理环境的集中管理，建立服务目录，提供服务门户，实现基于业务需求的资源规划、服务审批、使用计量、报表统计。
运维管理平台要求能满足大规模网络环境的统一管理的要求，实现对虚拟化环境、云计算平台和物理环境的监控和管理。
▲采用业界主流虚拟化技术；虚拟服务器的操作系统，需支持主流操作系统;虚拟服务器需支持主流中间件和数据库等软件产品。
▲能满足服务器动态扩展需求，当整个云平台资源不足时，新加的物理服务器资源可以被识别到，并加入到云平台的资源池中，而整个过程不要求停止原有服务，且不对原有服务造成影响。可实现对用户使用的资源如虚拟机、存储、IP、虚拟网络等资源的使用做到可视化、精细化管理并提供统计分析功能。
管理平台要求采用独立服务器设计，每个节点都可提供相要求的管理服务，任何单一节点故障都不会引起整个平台的管理中断。并且平台可提供分级分权的管理，针对不同的平台用户，可以各自使用和管理平台管理分配给的对要求资源，并且针对每种资源对象，可以部署更加精细化的权限管理和控制，极大满足了医卫云平台，构建云化 IT 架构中，多租户使用 IT 资源的灵活性。
平台可以根据企业云业务划分需求，可以将管理员划分为多级进行管理，不同的级别具有不同的管理权限和访问权限。
灾备
关键业务备份需求
关键业务是指各用户中数据变化频繁、对数据的敏感性高，不容许当前数据丢失的应用系统。关键业务对数据的灾备手段要求高，要求做到数据不丢失，一般要求使用实时备份策略，保证生产中心出现故障或数据损坏时，当前备份数据能能够快速恢复。本项目中的关键业务需要做本地灾备的是新公卫和 40 库。
要求如下：
▲要求 RPO ≈0，没有或基本没有数据丢失；RTO < 3 分钟，应用恢复时间在 30 分钟以内。
▲准实时复制无需停顿业务系统，适合 7X24 小时连续运行的业务系统。
▲无需主备系统硬件保证一致性，降低系统改造及投入的硬件成本。
▲对网络带宽消耗非常小，对业务系统性能影响小。
运维管理要求
云运维管理平台要求
云运维管理平台基本要求能支持分布式部署，可实现负载分担，满足大规模网络环境的统一管理的要求。业务管理要求能从业务维度对 IT 基础设施进行统一管理，直观展示业务的健康度、繁忙度、可用性。网络管理要求支持对多厂商设备状态及基本信息可以统一管理。可接受分析 syslog 日志，可以接受各类 SNMP trap 告警等。系统管理，可以支持主流操作系统的、数据库、中间件等的监控管理，并且可以自定义应用类型监控。可以对底层虚拟化及主机相关性能指标进行数据采集并监控。拓扑管理要求支持自动发现拓扑，支持 IP 拓扑、二层拓扑、自定义拓扑、可以展现机房、机柜、网络设备等情况,并且要求可以支持多种图表展示。包括 TopN、条形图、甘特图等。
▲提供统一的图形界面管理软件，可以在一个地点实现对虚拟化环境、云计算平台和物理环境的集中监控和管理，完成所有虚拟机的日常管理工作，包括控制管理、CPU 内存管理、用户管理、存储管理、网络管理、日志收集、性能分析、故障诊断、权限管理、在线维护等工作。
▲提供报表能力，实现对服务管理平台中各种信息的分析和呈现。
支撑系统要求当具有良好的扩展性，以适要求平台业务不断的发展；管理平台要求当具有良好的开放性，以适要求不同环境的管理要求。
▲要求有告警策略，并支持短信或邮件通知到管理员。
运维保障要求
投标人按照服务质量保证的服务标准要求提供各种售后服务，负责对其提供的服务进行维护或升级。
▲投标供应商应提供统一管理运维服务，运维人员需具备相关领域的认证资质或经验证明；投标人提供热线电话、电子邮件和在线网站等技术支持方式，提供 7*24 小时电话响应服务及 7*24 小时监控服务。做好资源管理工作、维护工作、统计工作、预警工作等。
▲配置实施及管理：进行云平台各软硬件设备的基础配置、IP 配置、角色用途、账号密码等的统一配置实施

及配置管理；为加强业务系统接入相关网络的安全管理工作，在不影响系统稳定运行的前提下，对账号、口令、授权、补丁、防护软件和防病毒软件、日志安全、服务与端口、启动项和自动播放功能、共享文件夹和文件系统、网络访问和会话超时等进行安全配置及更新。解决云平台相关问题，分析原因，做好记录。
▲节假日保障：重大节假日期间进行云平台运行和信息安全的重点保障。投标人提供 7*24 小时的现场运维服务，确保平台整体可用性。
故障处理和响应：投标人需对合同服务出现的故障响应做出相关保证。 提供 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。必须保证 1 小时之内响应、4 小时内派工程师到达现场、24 小时之内解决问题。应建立完善的私有云故障管理体系，管理体系涵盖故障处理的故障等级、职责分工和处理界面，每个处理流程必须留有电子化记录并在每个处理环节中落实到投标人的部门和相应的处理接口人。按照故障等级不同，需要有不同的处理时长和故障恢复时限。投标人要求按照 ITIL 或 ITSS 标准建设规范的运维组织和运维流程，并定制必要的故障管理、问题管理和变更管理等运维流程；并对各流程中涉及到的角色、职责、活动、策略等做出明确的定义。相关输出物为运维流程文档和运维规范。
日常监控、巡检：对医卫云平台进行日常监控、巡检，包括监控告警的处理，巡检异常的处理等；投标人需制定维护管理规定，并按照规定中的维护项目、周期和要求，制定详细的作业计划并执行。负责云平台内部系统安全的管理工作。做好平台优化并配合容灾应急工作。
平台故障处理：处理医卫云平台发生的各类软硬件、通信线路等故障，确保上层业务系统能够正常稳定运行；其中故障处理流程需要电子化并规定处理时限及当前处理环节的责任部门和责任人。
系统中断：投标人在中标后由于维护原因，需中断系统进行平台升级操作时，提前至少 72 小时（重大自然灾害除外）通知采购人做好相关准备工作，征得采购人同意方可实施。
投标人要求提供原厂绿色通道，重大事件或故障可直接由高级专家团队提供技术支持，快速响要求；高级专家团队技术领域要求覆盖云平台所涉及的服务器、存储、网络、安全、操作系统、云平台等各领域。
服务团队要求
▲投标人要求承诺提供本地化运维团队。投标人要求指派专门的项目经理或服务经理管理驻场人员。投标人要求提供经理名单。项目经理职责包括但不限于把控服务计划和实施进度、监督并提升服务交付质量、与客户沟通待协商问题、汇报工作里程碑、负责管理维护相关文档。
▲投标人必须保证按照合同核定的人数，进行人员配置，若出现有人员离职等情况，要求确保人员、工作的无缝衔接。合同期内，不得在招标人不同意的情况下，更换项目经理和驻场人员。
▲投标人要求在合同签订后的 1 个月内，落实全部人员到位。
▲运维服务团队中需具有 2 名高压电工操作专业认证，2 名低压电工操作专业认证，需提供相关证明材料。
项目验收要求
中标人应在项目完成时将系统的全部技术文件、资料列出清单，并依照清单向招标人提供全部技术文件，包括但不仅限于总体技术方案、设计、验收测试、用户使用说明、操作说明和系统常见故障分析等。
在项目实施完成之后，由招标人、监理、投标人等组成项目验收小组，完成项目验收工作。项目验收应当遵循的基本程序包括：制定项目验收办法，编制项目验收计划，确定系统验收范围，组织相关专家验收系统，编写项目验收报告等工作。
验收依据包括：招标文件、投标文件、采购合同及双方认可的其它约定。
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。培训计划应当符合以下要求：
（1）培训内容分为三类，分别为平台运行与维护管理培训和用户使用培训。通过培训应使各类用户能独立进行相应应用与管理、故障处理、日常维护等工作，确保系统能正常安全运行；
（2）投标单位应在投标文件中提出培训计划，计划包括培训项目、人数、地点等详细内容；
（3）投标人提供每年至少 1 次培训服务。

第四章　采购合同主要条款

包 1 合同模板：

合同通用条款及专用条款

合同统一编号： [合同中心-合同编码]

合同内部编号：

合同各方：

甲方：[合同中心-采购单位名称]	乙方：[合同中心-供应商名称]
地址：[合同中心-采购单位所在地]	地址：[合同中心-供应商所在地]
邮政编码：[合同中心-采购人单位邮编]	邮政编码：[合同中心-供应商单位邮编]
电话：[合同中心-采购单位联系人电话]	电话：[合同中心-供应商联系人电话]
传真：[合同中心-采购人单位传真]	传真：[合同中心-供应商单位传真]
联系人：[合同中心-采购单位联系人]	联系人：[合同中心-供应商联系人]

根据《中华人民共和国政府采购法》、《中华人民共和国民法典》之规定，本合同当事人在平等、自愿的基础上，经协商一致，同意按下述条款和条件签署本合同：

1．乙方根据本合同的规定向甲方提供以下货物或服务：

1．1 乙方所提供的货物或服务其来源应符合国家的有关规定，货物或服务的内容、要求、质量等按采购文件要求及投标承诺执行。

2．合同价格、履约地点和履约期限

2．1 合同价格

本合同价格为[合同中心-合同总价]元整（[合同中心-合同总价大写]）。

乙方为履行本合同而发生的所有费用均应包含在合同价中，甲方不再另行支付其它任何费用。

2．2 履约地点

按照采购文件的要求执行。

2．3 履约期限

履约期限：[合同中心-合同有效期]。

3．质量标准和要求

3．1 乙方所提供的货物或服务的质量标准按照国家标准、行业标准或制造厂家企业标准确定，上述标准不一致的，以严格的标准为准。没有国家标准、行业标准和企业标准的，按照通常标准或者符合合同目的的特定标准确定。

3．2 乙方所交付的货物或服务还应符合国家和上海市有关安全、环保、卫生之规定。

4．权利瑕疵担保

4．1 乙方保证对其交付的货物或服务享有合法的权利。

4．2 乙方保证在货物或服务上不存在任何未曾向甲方透露的担保物权，如抵押权、质押权、留置权等。

4．3 乙方保证其所交付的货物或服务没有侵犯任何第三人的知识产权和商业秘密等权利。

4．4 如甲方使用该货物或服务构成上述侵权的，则由乙方承担全部责任。

5．验收

5．1 根据合同的规定完成后，甲方应及时进行根据合同的规定进行验收。乙方应当以书面形式向甲方递交验收通知书，甲方在收到验收通知书后的 10 个工作日内，确定具体日期，由双方按照本合同的规定完成货物或服务验收。甲方有权委托第三方检测机构进行验收，对此乙方应当配合。

5．2 如果属于乙方原因致使系统未能通过验收，乙方应当排除故障，并自行承担相关费用，同时进行试运行，直至货物或服务完全符合验收标准。

5.3 如果属于甲方原因致使系统未能通过验收，甲方应在合理时间内排除故障，再次进行验收。如果属于故障之外的原因，除本合同规定的不可抗力外，甲方不愿或未能在规定的时间内完成验收，则由乙方单方面进行验收，并将验收报告提交甲方，即视为验收通过。

5．4 甲方根据合同的规定对货物或服务验收合格后，甲方收取发票并签署验收意见。

6．保密

6．1 如果甲方或乙方提供的内容属于保密的，应签订保密协议，甲乙双方均有保密义务。

7．付款

7．1 本合同以人民币付款（单位：元）。

7．2 本合同款项按照以下方式支付。

7．2．1 付款内容：按照采购文件约定的付款方式执行，采购文件未约定的，由甲乙双方协商确定。

7．2．2 付款条件：按照采购文件的要求执行。

8．甲方（甲方）的权利义务

8．1、甲方有权在合同规定的范围内享受，对没有达到合同规定的货物或服务质量或标准的服务事项，甲方有权要求乙方在规定的时间内加急提供货物或服务，直至符合要求为止。

8．2 如果乙方无法完成合同规定的货物或服务内容、或者货物或服务无法达到合同规定的货物或服务质量或标准的，造成的无法正常运行，甲方有权邀请第三方提供货物或服务，其支付的货物或服务费用由乙方承担；如果乙方不支付，甲方有权在支付乙方合同款项时扣除其相等的金额。

8．3 由于乙方货物或服务质量或延误的原因，使甲方有关或设备损坏造成经济损失的，甲方有权要求乙方进行经济赔偿。

8．4 甲方在合同规定的履约期限内有义务为乙方创造工作便利，并提供适合的工作环境，协助乙方完成工作。

8．5 当或设备发生故障时，甲方应及时告知乙方有关发生故障的相关信息，以便乙方及时分析故障原因，及时采取有效措施排除故障，恢复正常运行。

8． 6 如果甲方因工作需要对原有进行调整，应有义务并通过有效的方式及时通知乙方涉及合同货物或服务范围调整的，应与乙方协商解决。

9．乙方的权利与义务

9．1 乙方根据合同的货物或服务内容和要求及时提供相应的货物或服务，如果甲方在合同范围外增加或扩大服务内容的，乙方有权要求甲方支付其相应的费用。

9．2 乙方为了更好地进行服务，满足甲方对货物或服务质量的要求，有权利要求甲方提供合适的工作环境和便利。在进行故障处理紧急时，可以要求甲方进行合作配合。

9．3 如果由于甲方的责任而造成货物或服务延误或不能达到货物或服务质量的，乙方不承担违约责任。

9．4 由于因甲方工作人员人为操作失误、或供电等环境不符合合同设备正常工作要求、或其他不可抗力因素造成的设备损毁，乙方不承担赔偿责任。

9．5 乙方保证在履约中，未经甲方许可不得使用含有可以自动终止或妨碍系统运作的软件和硬件，否则，乙方应承担赔偿责任。

9． 6 乙方在履约时，发现存在潜在缺陷或故障时，有义务及时与甲方联系，共同落实防范措施，保证正常运行。

9．7 如果乙方确实需要第三方合作才能完成合同规定的货物或服务内容和服务质量的，应事先征得甲方的同意，并由乙方承担第三方提供货物或服务的费用。

9．8 乙方保证在履约中提供更换的部件是全新的、未使用过的。如果或证实服务是有缺陷的，包括潜在的缺陷或使用不符合要求的材料等，甲方可以根据本合同第 10 条规定以书面形式向乙方提出补救措施或索赔。

10．补救措施和索赔

10．1 甲方有权根据质量检测部门出具的检验证书向乙方提出索赔。

10．2 在履约期限内，如果乙方对提供货物或服务的缺陷负有责任而甲方提出索赔，乙方应按照甲方同意的下列一种或多种方式解决索赔事宜：

（1）根据货物或服务的质量状况以及甲方所遭受的损失，经过买卖双方商定降低货物或服务的价格。

（2）乙方应在接到甲方通知后七天内，根据合同的规定负责采用符合规定的规格、质量和性能要求的新零件、部件和设备来更换在货物或服务中有缺陷的部分或修补缺陷部分，其费用由乙方负担。

（3）如果在甲方发出索赔通知后十天内乙方未作答复，上述索赔应视为已被乙方接受。如果乙方未能在甲方发出索赔通知后十天内或甲方同意延长的期限内，按照上述规定的任何一种方法采取补救措施，甲方有权从应付的合同款项中扣除索赔金额，如不足以弥补甲方损失的，甲方有权进一步要求乙方赔偿。

11．履约延误

11．1 乙方应按照合同规定的时间、地点提供货物或服务。

11．2 如乙方无正当理由而拖延，甲方有权没收乙方提供的履约保证金，或解除合同并追究乙方的违约责任。

11．3 在履行合同过程中，如果乙方可能遇到妨碍按时提供货物或服务的情况时，应及时以书面形式将拖延的事实、可能拖延的期限和理由通知甲方。甲方在收到乙方通知后，应尽快对情况进行评价，并确定是否同意延期。

12．误期赔偿

12．1 除合同第 13 条规定外，如果乙方没有按照合同规定的时间提供货物或服务，甲方可以应付的合同款项中扣除误期赔偿费而不影响合同项下的其他补救方法，赔偿费按每（天）赔偿延期百分之零点五（0.5%）计收，直至提供货物或服务为止。但误期赔偿费的最高限额不超过合同价的百分之五（5%）。（一周按七天计算，不足七天按一周计算。）一旦达到误期赔偿的最高限额，甲方可考虑终止合同。

13．不可抗力

13．1 如果合同各方因不可抗力而导致合同实施延误或不能履行合同义务的话，不应该承担误期赔偿或不能履行合同义务的责任。

13．2 本条所述的“不可抗力”系指那些双方不可预见、不可避免、不可克服的事件，但不包括双方的违约或疏忽。这些事件包括但不限于：战争、严重火灾、洪水、台风、地震、国家政策的重大变化，以及双方商定的其他事件。

13．3 在不可抗力事件发生后，当事方应尽快以书面形式将不可抗力的情况和原因通知对方。合同各方应尽可能继续履行合同义务，并积极寻求采取合理的措施履行不受不可抗力影响的其他事项。合同各方应通过友好协商在合理的时间内达成进一步履行合同的协议。

14．履约保证金（采购文件有约定的按约定执行，未约定的本项不适用）

14．1 在本合同签署之前，乙方应向甲方提交一笔金额为元人民币的履约保证金。履约保证金应自出具之日起至全部货物或服务按本合同规定验收合格后三十天内有效。在全部货物或服务按本合同规定验收合格后 15 日内，甲方应一次性将履约保证金无息退还乙方。

14．2 履约保证金可以采用支票或者甲方认可的银行出具的保函。乙方提交履约保证金所需的有关费用均由其自行负担。

14．3 如乙方未能履行本合同规定的任何义务，则甲方有权从履约保证金中得到补偿。履约保证金不足弥补甲方损失的，乙方仍需承担赔偿责任。

15．争端的解决

15.1 合同各方应通过友好协商，解决在执行本合同过程中所发生的或与本合同有关的一切争端。如从协商开始十天内仍不能解决，可以向同级政府采购监管部门提请调解。

15．2 调解不成则提交上海仲裁委员会根据其仲裁规则和程序进行仲裁。

15．3 如仲裁事项不影响合同其它部分的履行，则在仲裁期间，除正在进行仲裁的部分外，本合同的其它部分应继续执行。

16．违约终止合同

16．1 在甲方对乙方违约而采取的任何补救措施不受影响的情况下，甲方可在下列情况下向乙方发出书面通知书，提出终止部分或全部合同。

（1）如果乙方未能在合同规定的期限或甲方同意延长的期限内提供部分或全部货物或服务。

（2）如果乙方未能履行合同规定的其它义务。

16．2 如果乙方在履行合同过程中有不正当竞争行为，甲方有权解除合同，并按《中华人民共和国反不正当竞争法》之规定由有关部门追究其法律责任。

17．破产终止合同

17．1 如果乙方丧失履约能力或被宣告破产，甲方可在任何时候以书面形式通知乙方终止合同而不给乙方补偿。该终止合同将不损害或影响甲方已经采取或将要采取任何行动或补救措施的权利。

18．合同转让和分包

18.1 除甲方事先书面同意外，乙方不得转让和分包其应履行的合同义务。

19．合同生效

19．1 本合同在合同各方签字盖章（采购文件要求提交履约保证金的，乙方需按要求提交履约保证金）后生效。

19．2 本合同一式份，甲乙双方各执一份。一份送同级政府采购监管部门备案。

20．合同附件

20．1 本合同附件包括： 招标(采购)文件、投标（响应）文件

20. 2 本合同附件与合同具有同等效力。

20. 3 合同文件应能相互解释，互为说明。若合同文件之间有矛盾，则以最新的文件为准。

21. 合同修改

21. 1 除了双方签署书面修改协议，并成为本合同不可分割的一部分之外，本合同条件不得有任何变化或修改。

签约各方：

甲方（盖章）：　　乙方（盖章）：

法定代表人或授权委托人（签章）：　　法定代表人或授权委托人（签章）：

日期：**[合同中心-签订时间]**　　日期：[合同中心-签订时间]

合同签订点:网上签约

第五章　评审办法

1. 单一来源采购人员将审查响应文件是否实质上响应了采购文件的要求。实质上响应的响应文件应该是与采购文件要求的全部条款、条件和规格相符，没有重大偏离的方案和响应。对关键条文的偏离、保留或反对，例如关于适用法律等的偏离将被认为是实质上的偏离。单一来源采购人员如发现响应人及其响应文件不符合本采购文件要求的，其响应文件将不列入评审范围。

2. 单一来源采购人员将按照前款规定，只对确定为实质上响应的响应文件进行评审。

3. 单一来源采购人员根据协商情况，在保证合理的成交价格及采购项目质量的前提下，确认成交。

4. 如果单一来源采购人员认为对采购文件作出实质性响应的响应人提供非合理的成交价格及采购项目质量无法满足采购需求的，则单一来源采购人员可对本次采购进行否决。

第六章　响应文件格式及附件

附件 1　　MCGS1001

1 响 应 函

致：采购人名称

上海市闵行区政府采购中心

根据贵方为（项目名称）项目单一来源采购货物及服务的采购邀请（项目编号）签字代表（姓名、职务）经正式授权并代表响应人（响应人名称）提交响应文件。电子响应文件按照电子采购平台规定提交。

据此函，签字代表宣布同意如下：

1. 我方已审阅、正确理解了采购文件的全部内容，并完全接受且执行采购文件中规定响应人所履行的各项义务。
2. 我方对所附报价一览表中规定的应提供和交付的货物及服务报价总价为：
（大写）人民币（元）整，（小写）人民币（元）　整。
3. 我方将按采购文件的规定和要求履行合同的责任和义务。
4. 我方自递交响应文件截止时间之日起响应有效期为 90 天。
5. 我方同意提供按照贵方可能要求的与其报价有关的一切数据或资料，完全理解贵方不一定要接受最低价的报价或收到的任何报价。
6. 我方承诺与买方聘请的为此项目提供咨询服务的公司及任何附属机构均无关联，我方不是买方的附属机构。
7. 我方同意按照《政府采购法》及相关法律法规的规定提出询问或质疑。我方已经充分行使了对采购文件提出质疑和澄清的权利，因此我方承诺不再对采购文件提出质疑。
8. 与本次采购有关的一切正式往来信函请寄：

响应人全称：

地　址：＿＿＿＿＿＿＿＿＿＿＿＿　邮　编：＿＿＿＿＿＿

电　话：＿＿＿＿＿＿＿＿＿＿＿＿　传　真：＿＿＿＿＿＿

法定代表人或授权代表（签字或盖章）：＿＿＿＿＿

响应人签署日期：＿＿＿＿＿＿

响应人公章：

附件 2　　MCGS1002

2　响应人声明函

（公司名称）参加本（项目名称）政府采购活动，在此郑重承诺

一、　本公司不存在下列各项情形：

1. 为本采购项目前期准备或者监理工作直接或间接提供设计、咨询服务的法人、其他组织及其附属机构；
2. 与采购方或采购代理方存在隶属关系；
3. 为本项目的监理人；
4. 为本项目提供采购代理服务；
5. 与本项目的监理人或采购代理机构同为一个法定代表人；
6. 与本项目的监理人或采购代理机构相互控股或参股；
7. 与本项目的监理人或采购代理机构相互任职或工作；
8. 被责令停业；
9. 财产被接管或冻结；
10. 被政府采购监管部门处罚并在处罚有效期内被禁止参加政府采购的。

二、　采购文件的疑点及异议

本公司仔细阅读了本项目采购文件（包括补充文件，以下同）所有条款，认为本采购文件要求明确，同时未存在以不合理条件限制、排斥潜在响应人或者响应人的倾向性、排他性条款。本公司对本采购文件所有条款没有疑点及异议。

三、　采购文件的实质性响应

本公司仔细审核了本项目采购文件及准备递交的响应文件，认为本响应文件已不存在任何疏漏和偏差，实质性响应了本项目采购文件的要求。本公司不会就采购文件是否存在非实质性响应内容而声明本公司响应文件应该被废标，并以此依据提出质疑或投诉。

本公司认可采购文件、成交人响应文件、合同前按时间排序的符合法规的补充文件、合同后按时间排序的符合法规的补充文件均为合同的强制性附件，合同文本及补充协议与成交人的响应文件有冲突的，以成交人的响应文件相关承诺为准。

不论响应文件和合同及补充协议是否对采购文件中与合同相关条款作修改、遗漏、补充、变更或否决，本公司认可采购文件中与合同相关条款始终为合同履行全过程具有不可更改，强制约束的条款。

四、　项目主要工作人员

1. 本公司委派☐**法定代表人**☐**组织负责人**☐**法定代表人授权委托人**（姓名），全权代表本公司参加采购流程环节的事务工作，详见响应文件“法定代表人授权书”。
2. 本公司若成交，将派遣☑**项目负责人**☐**注册建造师（项目经理）**（姓名）负责本项目的履约工作。

响应人名称（响应人章）

日期：

附件 3　　MCGS1003

3　法定代表人授权书

本授权书声明：注册于（公司地址）的（公司名称），（法定代表人）授权（被授权人的姓名、职务）代表本公司为本公司的合法和全权代表人，就（项目名称）项目谈判(报价)、合同谈判和执行、完成的全过程，以本公司名义处理一切与之有关的事务。

本授权书于____年____月____日签字有效，特此声明。

法定代表人（签字或盖章）：

响应人名称（公章）：

被授权人（签字或盖章）：

被授权人身份证正面	被授权人身份证反面

附件 4　　MCGS1004

4 报价一览表

上海市闵行区卫建委医卫云运维服务项目（2023 运维）包 1

服务内容	服务期限	金额(总价、元)

附件 5　　MCGS1005

5　廉政承诺书

兹我单位于参加　（项目名称）　项目招标前作如下郑重承诺：

我单位将遵守国家法律、法规、规章，以及闵行区政府采购（招标投标）相关制度，自觉遵守政府采购（招标投标）市场次序，自觉抵制各种不良行为，恪守公平竞争原则，认真负责、诚实守信地参加政府采购（招标投标）活动。

通过正常途径开展相关工作，不为谋取某些不正当利益而向采购（招标）单位和个人、评标委员会赠送礼金、礼品、有价证券和贵重物品和为其购置与提供通讯工具、交通工具、家电、办公用品等钱物，或者邀请其外出旅游和进入营业性娱乐场所。

诚信履行合同，不为谋取不正当利益擅自与采购（招标）单位工作人员就工程承包、工程费用、材料设备供应、工作量变动、工程验收、工程质量问题处理，以及货物和服务采购的验收、质量问题处理、售后服务等进行私下商谈或者达成默契。

若违背上述承诺，我单位接受闵行区政府采购监管部门依法给予处理，并承担相应的法律责任，若造成采购（招标）单位损失的，愿承担相应的赔偿责任。

承诺单位（公章）：

日期：

附件 6　　MCGS1006

（非残疾人福利性单位无需提供此函）

6　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。

单位名称（盖章）：

日　期：

7 财务状况及税收、社会保障资金缴纳情况声明函

我方（供应商名称）符合《中华人民共和国政府采购法》第二十二条第一款第（二）项、第（四）项规定条件，具体包括：

1. 具有健全的财务会计制度；

2. 有依法缴纳税收和社会保障资金的良好记录。

特此声明。

我方对上述声明的真实性负责。如有虚假，将依法承担相应责任。

供应商名称（公章）

日期：

附件 8 MCGS1008

8 中小企业声明函

中小企业声明函（货物）

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（单位名称）的（项目名称）采购活动，提供的货物全部为符合政策要求的中小企业制造。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）；制造商为（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）；

2. （标的名称），属于（采购文件中明确的所属行业）；制造商为（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。

企业名称（盖章）：

日期：

备注：[1]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。

中小企业声明函（工程、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（单位名称）的（项目名称）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[1]，属于（中型企业、小型企业、微型企业）；

2. （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。

企业名称（盖章）：

日期：

备注：[1]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。

附件 9 MCGS1009

9 三年内在经营活动中没有重大违法记录的书面声明

在参加本次投标之日起前三年内，我公司未因违法经营受到刑事处罚或者责令停产停业、吊销许可证或者执照、较大数额罚款等行政处罚。

特此声明。

承诺单位（公章）：

日期：

附件 10

10 各分项货物、服务报价一览表

（响应人可根据项目情况自行编制表格）

响应人名称：_____ 项目名称：_____ 项目编号：

序号	分项名称	综合单价（元）	小计（元）	偏离程度	证明材料
				*	*
				*	*
				*	*

我们承诺本表中技术规格偏离的内容真实有效，无任何虚假之处，并且愿意承担因不满足此承诺而引起的相应的法律责任并接受相关部门的处罚。

响应人：（公章）

法定代表人或授权代表：（签字或签章）

注：1、本表请按照采购文件设备清单参数要求逐条编制。

2、偏离程度请填写“正偏离、负偏离或无偏离”字样。

3、证明资料请填写**“见响应文件第*页”**字样，具体证明材料例如：图片、厂家说明书。

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；单价金额小数点有明显错位的，应以总价为准，并修改单价

附件 11

11 详细货物、服务情况一览表

（响应人可根据项目情况自行编制表格）

项目编号：_____ 项目名称：_____

序号	货物、服务名称、	服务内容、货物的品牌型号规格等	详细说明	备注
（货物）交货期：合同签定之日起_____个日历日（工作日），质保期____月。 （服务）服务期：				

响应人：（公章）

法定代表人或授权代表：（签字或签章）_____

附件 12

12 技术响应/偏离表

（响应人可根据项目情况自行编制表格）

项目编号：_____ 项目名称：_____

合同包	响应的产品、服务名称	采购文件的货物或服务要求	投标货物参数或投标服务的内容	正偏离还是负偏离	偏离详细说明

注：响应人提交的响应文件中与采购文件的技术部分的要求有不同时，应逐条列在偏离表中。

响应人：（公章）

法定代表人或授权代表：（签字或签章）

附件 13

13 商务条款响应/偏离表

响应人名称：_____ 项目编号：_____

序号	采购文件条目号	采购文件的商务条款	响应文件的商务条款	说明
	响应人资格要求			
	……			
	……			
	……			
	无效标条款 1			
	无效标条款 2			
	……			
	……			

响应人：（公章）

法定代表人或授权代表：（签字或签章）

附件 14

14 项目负责人基本情况表

响应人名称：_____ 项目编号：_____

姓名		出生年月		文化程度		职务	
最高学历毕业院校时间和专业			从事相关工作年限			联系方式	
执业资格及获得年限			技术职称及获得年限			学位	
主要工作经历							
时间	工作单位		所属部门	担任职务		证明人	联系电话

响应人：（公章）

法定代表人或授权代表：（签字或签章）

附件 15

15 针对本项目拟委派所有人员情况表

响应人名称：_____ 项目编号：_____

序号	姓名	性别	出生年月	文化程度	职 称等级	从事专业	成功案例项目	本项目中职务
								项目负责人
								其他人员

响应人：（公章）

法定代表人或授权代表：（签字或签章）_____

附件 16

16 服务提供者的资格声明

1. 名称及其他情况

1) 服务提供者名称：
2) 地址：
3) 成立和（或）注册日期：
4) 主管部门：
5) 企业性质：
6) 职员人数：
   （a） 一般工人：
   （b） 技术人员：
7) 近期资产负债表（到　　年　　月　　日止）
   （c） 固定资产：
      （i） 原值：
      （ii） 净值：
   （d） 流动资金：
   （e） 长期负债：
   （f） 短期负债：
   （g） 资金来源：
      （i） 自有资金：
      （ii） 银行贷款：
   （h） 资金类型：
      （i） 生产资金：
      （ii） 非生产资金：

2. 服务提供者提供此类服务的历史（年数）

_____

_____

3. 近三年的年营业额

年份	总额
_____	_____
_____	_____

4. 有关开户银行的名称和地址

银行名称 地址

5. 其他情况

兹证明上述声明是真实、正确的，并提供了全部能提供的资料和数据，我方同意遵照贵方要求出示有关证明文件。

日期：

服务提供者名称：

授权代表签字：

授权代表的职务：

电话号码：

传真号码：

电子信箱：

公章：

附件 17

17 政府采购供应商不良行为内容

1．提供虚假材料的；

2．采取不正当手段诋毁、排挤其他供应商的；

3．与采购人、其他供应商或者集中采购机构恶意串通的；

4．以他人名义投标或承接项目的；

5．在招标投标过程中与采购人进行协商谈判的；

6．开标后擅自撤销投标，影响招标继续进行的；

7．以向采购人、评标委员会成员行贿等不正当手段谋取中标的；

8．中标、成交后无正当理由拒绝签订政府采购合同的；

9．将中标项目转让给他人或将中标项目肢解后分别转让给他人；

10．无正当理由拒绝履行合同的；

11．故意提供假冒伪劣产品或走私物品的；

12．拒绝提供售后服务或者服务质量存在重大问题给采购人造成损害的；

13．恶意投诉，给采购人或者集中采购机构造成损害的；

14．恶意哄抬或压低价格的；

15．合同单价明显高于同类产品同期市场平均价的；

16．单项合同毛利率上限超过服务协议中规定的毛利率上限的（特指公务外出（国外）定点服务项目）；

17．违反《中华人民共和国价格法》中相关规定的；

18．拒绝有关部门监督检查或者提供虚假情况的；

19．区财政局认定的其他有违诚实信用的行为。

若发现政府采购供应商有以上不良行为的，将报请有关部门处理。

附件 18

工业和信息化部　国家统计局
国家发展和改革委员会　财政部
关于印发中小企业划型标准规定的通知

工信部联企业〔2011〕300 号

各省、自治区、直辖市人民政府，国务院各部委、各直属机构及有关单位：

为贯彻落实《中华人民共和国中小企业促进法》和《国务院关于进一步促进中小企业发展的若干意见》（国发〔2009〕36 号），工业和信息化部、国家统计局、发展改革委、财政部研究制定了《中小企业划型标准规定》。经国务院同意，现印发给你们，请遵照执行。

工业和信息化部　　国家统计局

国家发展和改革委员会　　财政部

二〇一一年六月十八日

中小企业划型标准规定

一、根据《中华人民共和国中小企业促进法》和《国务院关于进一步促进中小企业发展的若干意见》（国发〔2009〕36 号），制定本规定。

二、中小企业划分为中型、小型、微型三种类型，具体标准根据企业从业人员、营业收入、资产总额等指标，结合行业特点制定。

三、本规定适用的行业包括：农、林、牧、渔业，工业（包括采矿业，制造业，电力、热力、燃气及水生产和供应业），建筑业，批发业，零售业，交通运输业（不含铁路运输业），仓储业，邮政业，住宿业，餐饮业，信息传输

业（包括电信、互联网和相关服务），软件和信息技术服务业，房地产开发经营，物业管理，租赁和商务服务业，其他未列明行业（包括科学研究和技术服务业，水利、环境和公共设施管理业，居民服务、修理和其他服务业，社会工作，文化、体育和娱乐业等）。

四、各行业划型标准为：

（一）农、林、牧、渔业。营业收入 20000 万元以下的为中小微型企业。其中，营业收入 500 万元及以上的为中型企业，营业收入 50 万元及以上的为小型企业，营业收入 50 万元以下的为微型企业。

（二）工业。从业人员 1000 人以下或营业收入 40000 万元以下的为中小微型企业。其中，从业人员 300 人及以上，且营业收入 2000 万元及以上的为中型企业；从业人员 20 人及以上，且营业收入 300 万元及以上的为小型企业；从业人员 20 人以下或营业收入 300 万元以下的为微型企业。

（三）建筑业。营业收入 80000 万元以下或资产总额 80000 万元以下的为中小微型企业。其中，营业收入 6000 万元及以上，且资产总额 5000 万元及以上的为中型企业；营业收入 300 万元及以上，且资产总额 300 万元及以上的为小型企业；营业收入 300 万元以下或资产总额 300 万元以下的为微型企业。

（四）批发业。从业人员 200 人以下或营业收入 40000 万元以下的为中小微型企业。其中，从业人员 20 人及以上，且营业收入 5000 万元及以上的为中型企业；从业人员 5 人及以上，且营业收入 1000 万元及以上的为小型企业；从业人员 5 人以下或营业收入 1000 万元以下的为微型企业。

（五）零售业。从业人员 300 人以下或营业收入 20000 万元以下的为中小微型企业。其中，从业人员 50 人及以上，且营业收入 500 万元及以上的为中型企业；从业人员 10 人及以上，且营业收入 100 万元及以上的为小型企业；从业人员 10 人以下或营业收入 100 万元以下的为微型企业。

（六）交通运输业。从业人员 1000 人以下或营业收入 30000 万元以下的为中小微型企业。其中，从业人员 300 人及以上，且营业收入 3000 万元及以上的为中型企业；从业人员 20 人及以上，且营业收入 200 万元及以上的为小型企业；从业人员 20 人以下或营业收入 200 万元以下的为微型企业。

（七）仓储业。从业人员200人以下或营业收入30000万元以下的为中小微型企业。其中，从业人员100人及以上，且营业收入1000万元及以上的为中型企业；从业人员20人及以上，且营业收入100万元及以上的为小型企业；从业人员20人以下或营业收入100万元以下的为微型企业。

（八）邮政业。从业人员1000人以下或营业收入30000万元以下的为中小微型企业。其中，从业人员300人及以上，且营业收入2000万元及以上的为中型企业；从业人员20人及以上，且营业收入100万元及以上的为小型企业；从业人员20人以下或营业收入100万元以下的为微型企业。

（九）住宿业。从业人员300人以下或营业收入10000万元以下的为中小微型企业。其中，从业人员100人及以上，且营业收入2000万元及以上的为中型企业；从业人员10人及以上，且营业收入100万元及以上的为小型企业；从业人员10人以下或营业收入100万元以下的为微型企业。

（十）餐饮业。从业人员300人以下或营业收入10000万元以下的为中小微型企业。其中，从业人员100人及以上，且营业收入2000万元及以上的为中型企业；从业人员10人及以上，且营业收入100万元及以上的为小型企业；从业人员10人以下或营业收入100万元以下的为微型企业。

（十一）信息传输业。从业人员2000人以下或营业收入100000万元以下的为中小微型企业。其中，从业人员100人及以上，且营业收入1000万元及以上的为中型企业；从业人员10人及以上，且营业收入100万元及以上的为小型企业；从业人员10人以下或营业收入100万元以下的为微型企业。

（十二）软件和信息技术服务业。从业人员300人以下或营业收入10000万元以下的为中小微型企业。其中，从业人员100人及以上，且营业收入1000万元及以上的为中型企业；从业人员10人及以上，且营业收入50万元及以上的为小型企业；从业人员10人以下或营业收入50万元以下的为微型企业。

（十三）房地产开发经营。营业收入200000万元以下或资产总额10000万元以下的为中小微型企业。其中，营业收入1000万元及以上，且资产总额5000万元及以上的为中型企业；营业收入100万元及以上，且资产总额2000万元及

以上的为小型企业；营业收入100万元以下或资产总额2000万元以下的为微型企业。

（十四）物业管理。从业人员1000人以下或营业收入5000万元以下的为中小微型企业。其中，从业人员300人及以上，且营业收入1000万元及以上的为中型企业；从业人员100人及以上，且营业收入500万元及以上的为小型企业；从业人员100人以下或营业收入500万元以下的为微型企业。

（十五）租赁和商务服务业。从业人员300人以下或资产总额120000万元以下的为中小微型企业。其中，从业人员100人及以上，且资产总额8000万元及以上的为中型企业；从业人员10人及以上，且资产总额100万元及以上的为小型企业；从业人员10人以下或资产总额100万元以下的为微型企业。

（十六）其他未列明行业。从业人员300人以下的为中小微型企业。其中，从业人员100人及以上的为中型企业；从业人员10人及以上的为小型企业；从业人员10人以下的为微型企业。

五、企业类型的划分以统计部门的统计数据为依据。

六、本规定适用于在中华人民共和国境内依法设立的各类所有制和各种组织形式的企业。个体工商户和本规定以外的行业，参照本规定进行划型。

七、本规定的中型企业标准上限即为大型企业标准的下限，国家统计部门据此制定大中小微型企业的统计分类。国务院有关部门据此进行相关数据分析，不得制定与本规定不一致的企业划型标准。

八、本规定由工业和信息化部、国家统计局会同有关部门根据《国民经济行业分类》修订情况和企业发展变化情况适时修订。

九、本规定由工业和信息化部、国家统计局会同有关部门负责解释。

十、本规定自发布之日起执行，原国家经贸委、原国家计委、财政部和国家统计局2003年颁布的《中小企业标准暂行规定》同时废止。