**杭州市政协机房设备维保项目招标文件**

杭州市政协办公厅

二〇一六年十一月

**目 录**

第一部分 招标公告

第二部分 编制和提交采购响应文件须知

第三部分 项目技术规范和服务要求

第四部分 评标办法

**第一部分 招标公告**

杭州市政协办公厅就“机房设备维保项目”进行公开招标采购。具体如下：

1、招标编号：HZZX-2016-0002

 2、项目名称：杭州市政协机房设备运维服务项目。

3、招标内容：采购内容主要以下几个方面：分别是机房服务器监控软件一套；内网杀毒软件一套；机房服务器硬件运维；Windows server、Oracle、SQL server、杀毒等系统及应用软件的维护升级服务工作。

4、合格的投标人应具备的资格要求：在中华人民共和国境内注册，具有独立法人资格，符合《中华人民共和国政府采购法》第二十二条的规定，且符合、承认并承诺履行本招标文件各项规定，所提供的货物和服务须在我国境内合法销售的。

5、采购方式：单位组织招标

6、开标时间与地点：2016年11月30日下午3时00分，地点：杭州市江干区解放东路18号市民中心B座2313会议室。

7、项目联系方式：杭州市政协机关信息中心，联系人：夏工， 联系电话：0571-85259355，传真：0571-85259355。

 8、本项目非依法必招项目，参照政府采购有关程序操作。对时间安排和采购文件条款有异议，请在投标截止时间之前七天书面向招标人提出。

**第二部分 编制和提交采购响应文件须知**

|  |  |
| --- | --- |
| 条款 | 内容规定 |
| 1 | 项目名称：杭州市政协机房设备运维服务项目 |
| 2 | 采购内容：机房服务器监控软件一套；内网杀毒软件一套；机房服务器硬件运维；Windows server、Oracle、SQL server、杀毒等系统及应用软件的维护升级服务工作。 |
| 3 | 项目实施地点：杭州市政协托管机房（华数机房）。 |
| 4 | 要求质量标准: 规范、专业、可靠、及时、全面。所提供服务须符合国家技术规范和质量标准，并符合采购人的采购要求。本采购适用于杭州市政府采购中心规则。 |
| 5 | 主要技术参数和性能要求：详见第三部分——项目技术规范和服务要求。 |
| 6 | 本项目采购预算为人民币十万元 |
| 7 | 项目服务时间：一年 |
| 8 | 应标截止时间：2016年11月28日下午3时30分。 |
| 9 | 应标文件递交至单位：杭州市政协机关信息中心应标文件递交至地点：杭州市江干区解放东路18号市民中心B座2419室 |
| 10 | 开标时间：2016年11月30日下午3时00分；开标地点：杭州市江干区解放东路18号市民中心B座2313室 |
| 12 | 技术支持期：在服务期内，提供多种方式的运行技术支持。 |
| 13 | 合同名称 | 《杭州市政协机房设备运维服务项目合同》 |
| 14 | 投标有效期：自投标截止日起30天。如采购单位认为必要，可延长至总计最长不超过60天。 |
| 15 | 投标文件：各公司根据招标文件内容自行编写：报价、公司资信和技术响应文件装订1正本3副本文件。 |

**第三部分 项目技术规范和服务要求**

一、采购内容：

采购内容主要分为几个方面，分别是机房服务器监控软件一套；内网杀毒软件一套；服务器硬件运维；Windows server、Oracle、SQL server、杀毒软件等系统及应用软件的维护升级工作。

1、服务器监控软件一套

|  | 指标项 | 主要技术参数描述 |
| --- | --- | --- |
| IT运维监控综合管理平台 | 品牌要求 | 国内知名品牌；软件生产厂家必须具有软件企业认定证书。软件生产厂家必须通过ISO9000质量管理体系认证。软件产品必须具有软件产品登记证书。软件产品必须具有计算机软件著作权证书。【提供证书复印件，原件备查。】 |
| 总体要求 | 为了更好的兼容各个品牌设备，投标产品为第三方纯软件平台 |
| 系统软件基于B/S架构，全WEB管理、中文界面；支持分布式部署，支持远程监控管理。 |
| 中文界面，符合一般操作习惯。系统界面友好，以左边模块树形结构和右边展现效果的排版视图。 |
| 二次开发：系统具有标准的开放接口，能够满足用户后续二次开发的需求，根据厂商提供的协议快速进行二次开发部署。 |
| 开放性：具有很好的开放性，支持业界标准，具备通过集成设备厂商网管软件及通过各厂商网管系统开放的API端口对其设备进行网管的功能；系统采集的系统运行及报警数据可以通过如XML、文本、数据库接口等各种方式输出到第三方系统。 |
| 功能总体要求 | 在统一平台上实现IT基础网络、操作系统、存储、虚拟机、数据库、中间件和应用服务、应用系统等监测，实现统一的报警管理。系统软件基于B/S架构。全IP设置：环境采集器和所有的串口装置均转换为IP接口。系统支持自定义拓扑图功能，提供多种视图的展现。不同设备可灵活配置不同的采集周期。在监控过程中发生的事件，通过报警平台，以短信、电话、邮件、语音和声光等多种方式报警。系统同时提供设备资产管理、故障管理、巡检管理等运维功能管理模块。可通过web配置、管理和查看设备运行状态；可查询设备各监控指标历史监控记录的曲线图、柱状图、饼图等详细信息；可自定义生成各种形式的报表，同时可将报表发送邮件给指定的邮箱；可针对任何监控指标灵活设置多级报警策略；可设置手机短信、电子邮件、电视墙、颜色、声音等多种报警方式。全WEB管理、中文界面；集中监控跨平台操作系统：Windows、Linux、AIX、HP-Unix、Solaris、FreeBSD、VMWare等系统；集中监控数据库，比如：Oracle、DB2、SQL Server、MySQL、PostgreSQL；集中监控应用服务器与WEB服务器：Apache、Tomcat、JBoss、Resin、WebLogic、WebSphere等应用服务器与软件； 集中监控任意进程；集中监控硬件信息：CPU温度监控、磁盘温度监控、硬盘温度监控；按主机、按应用监控；可以随意定制实时状态查询图、项目集；完善的报表统计功能，可自定义各种形式报表；智能的历史数据分析功能，强大的二次开发数据接口与性能收集接口；报表统计分析功能:可查看任意旪间段报表，满足不同级别用户和管理者的需求；可生成设备性能横向、纵向对比曲线图和报表。对各种性能的监控，用户都可以通过个性化设置生成所需要的报表，如曲线图，柱状图，对比分析图等；可通过对不同的设备的同一种性能进行比较，判断设备的负载。报告具有WORD\HTML格式，可以外发、上传给上级主管人员。可设置按月、周、日自动生成报表发送到指定邮箱。自动与VISIO集成。与VISIO图络图、机架图的无缝结合，使用现有的VISIO图与软件集成后即可自动实现VISIO图中显示各种设备的状态。与其他系统无缝集成，可与第三方软件无缝集成，为客户现有系统及将来新增系统有效对接。在整个监控过程中，系统分为三个层次：第一层：数据采集层。根据设定采集周期，采集机房环境、动力设备、网络设备、操作系统、存储、虚拟机、数据库、安全工具、中间件和应用服务、应用系统等关键监测指标数据，实时传递给数据处理系统。第二层：数据处理层。当数据处理系统接收到采集数据后，将采集数据进行一定的检查和判断，将产生报警事件发送到应用层，在WEB值班工作站显示报警警示信息。同时根据报警配置情况。通过短信、电话、邮件、语音和声光实时报警，相关人员及时收到报警信息，在第一时间及时处理。第三层：数据展现层。它是一个完整的管理平台，从多方面多视角动态展现各类视图，包括IT构架监控管理视图、机房监控管理视图、业务服务监控管理视图，动态实时展示各类监测数据，以丰富的柱状图、曲线图、饼图等图形和表格，表现实时监测数据和历史监测数据、统计数据，而且具有事件报表查询和自定义、监测设备和指标的配置、各类报警的配置、值班配置，以及设备资产管理、故障管理、巡检管理等运维功能，具有完善安全管理，满足不同用户的管理需求。 |
| 支持授权 | 至少支持300台IT设备的监控，包括网络设备、安全设备等。存储管理支持100T容量的不区分品牌的管理。虚拟化管理支持30台虚拟机管理。支持服务器30各类服务器支持数据库10套以上，不限于SQL，Oracle等数据库；配置短信报警1套，可支持多系统统一报警 |
| 综合数据展现功能 | 系统应该能够提供综合数据展现功能，集中展示各类统计/实时数据。可以根据业务模型灵活展现业务系统、业务服务与IT组件之间的关系。支持应用视图、链路视图、位置视图等全局汇总及明细视图管理与展示。支持业务浏览视图的自定义。支持层次化的监视视图展示。 |
| 系统提供自定义功能，根据房间的实际布局，摆放各种监测对象图标，这些图标均能实时反映设备的运行情况和监测数据。 |
| 支持机房及机柜视图管理与展示，可直观真实的显示机房、机柜实时运行状况（提供产品截图） |
| 提供可定制的实时值班监控页面，可定义各类实时数据分类，包括网络设备性能排行，主机性能排行、服务可用性一览，业务运行统计数据，自定义指标实时数据等。 |
| 故障管理功能 | 支持多种的告警方式，如手机短信、电话语音、声光、电子邮件等；可灵活设置各类指标报警阀值，可分多个报警等级。支持远程语音、短信告警信息查询；短信报警方式，可支持多种如短信猫，短信平台、WEBSERVICES等；支持批量配置告警，支持故障原因关联分析；。告警操作功能：可以对告警进行清除告警、生成导出告警报表等操作。告警订阅功能：告警订阅允许用户定制自己关心的告警。当指定告警发生时，系统将告警信息以短信、语音、声光或Email的形式发送给指定用户。 |
| 支持IP管控功能 | 支持IP地址分布视图，帮助用户快速规划整理IP地址，查询某地址段设备的PING通状态，以此可监控到手持终端设备是否在线工作。 |
| 网络设备管理功能 | 软件具备主流管理设备能力，支持异构网络统一管理，至少支持交换机、路由器、交换路由器、防火墙、UPS、IP节点等网络设备的监控；并可自动识别设备间的线路，并对线路性能进行监控。 |
| 拓扑管理 | 可通过搜索自动生成设备拓扑图，拓扑图美观大方。 |
| 支持折线的拓扑图连接方式。 |
| 支持自动切换到机房管理模块中的设备位置。 |
| 面板管理功能 | 可对交换机的真实面板进行管理，面板图必须与交换机厂家真实面板图一致。（提供产品截图） |
| 网络性能管理功能 | 性能管理功能主要面向各类网络设备的性能综合监测和分析，应具有性能监测管理、性能数据上报管理、性能数据管理、性能门限管理、性能分析等子功能。 |
| 可在网络总拓扑图上通过点击设备或右键直接浏览设备状态并集成远程Telnet接口检测、Web接口检测、Ping测试，SNMP连接测试，TraceRoute等工具。 |
| 系统必须支持分布式数据采集，可以将不同网段范围的设备的性能数据交由不同服务器上的数据采集系统进行采集，并集中提供网管系统处理和访问； |
| 系统必须能适应不同取数间隔，自动重用已获得的性能数据，避免大量重复取数造成的网络资源浪费； |
| 系统必须提供SNMPOID方式能够把需要的性能数据提取出来做历史记录。 |
| 支持网络设备的ARP表、MAC表、路由表等表格数据定期存储，差异自动比对； |
| 提供设备Vlan信息，并可简单直接配置Vlan配置。 |
| 主机性能管理功能 | 提供对Windows、IBMAIX、SUNSolaris、HP-UNIX、Linux、CentOS、NovellSuse、FreeBSD操作系统实现监控管理 |
| 支持主机运行的实时参数显示； |
| 支持主机一体化展现图.可以在一张图上展现主机日志、主机的应用使用情况； |
| 可通过纯软件方式直接对设备硬件进行可视化，图形化管理。 |
| 可在主机管理的一体化图中，体现设备的资产情况，包括资产的服务期、负责人、联系方式等。 |
| 主机日志管理功能 | 需要支持window、Linux的服务器上各种文本日志的监控； |
| 支持日志文件增量比对，获取符合包含关键字的异常信息获取； |
| 应该可配置各种监控指标，当指标异常超过一定比率后，提醒用户并给出处理建议； |
| 数据库性能管理功能 | 系统提供ORACLE、MSSQL、MySQL、SYBASE、DB2等数据库的监测。监测连接时间、例程名、例程开始时间、归档日志模式、buffer cache击中率、锁数量、死锁数量、当前连接事务数、等待事务数、内存、用户连接、请求、数据库、进程，以及用户自定义等指标。 |
| 中间件监测 | 支持对目前广泛使用的Tuxedo、Websphere、WebLogic中间件的监测；监测内容至少包括：基本配置信息、运行状态、JVM堆栈监测、连接监测、JTA事务状况监测、WEB应用监测指标、Servlet监测指标、EJB监测等 |
| 虚拟机的监测 | 既可以对独立的ESXi宿主机进行监控，也支持对集成的vCenter进行监控，监控主要从下面三个层次进行：宿主机层面，对VMware宿主机（Host）的CPU、内存、磁盘和网络等项目进行监测；虚拟机层面，对VMware宿主机上面安装的每个虚拟机（Virtual Machine）的CPU、内存、磁盘和网络进行监测；存储层面，对VMware 的每个存储的使用率，剩余量、总容量指标进行监测。 |
| 公共服务监测 | HTTP/ HTTPS服务管理：监测HTTP/ HTTPS服务的运行状况，包括端口和服务是否正常，计算主页存活率，并且可以对HTTP/ HTTPS返回的结果进行分析，判断服务器的实际工作是否正常。FTP服务管理：监测FTP服务器的工作状态。在判断条件中可以选择是否允许匿名登录、验证登录、验证文件是否存在等。SMTP服务管理：监测邮件发送服务器的工作状态。POP3服务管理：监测邮件接收服务器的工作状态，包括邮件数量和邮箱使用量。DNS服务：监测DNS服务的运行，DNS服务的延时及服务的正确性。Apache服务：监测Apache服务器的CPU负载，Apache运行时间、每分钟的请求、每秒处理字节数、繁忙作业数、空闲作业数等。 |
| 应用系统监测 | 支持应用系统监控的二次开发。应用系统信息的采集分成四个部分：一是进程信息的采集，为了保证企业的各个系统运行正常，系统组成的各项进程需要进行监控，包括是否运行，进程的个数，进程消耗的资源等信息；二是系统本身的日志，大多数应用系统提供了日志输出功能，将自己的运行信息通过文本文件的格式或者是数据库的形式传递出来，采集到这些信息，进而判断系统的运行状态；三是系统关键数据的判断，这种信息的判断，可以针对不同的系统开发数据代理。四 支持通过仿真客户端登陆的方式验证后台服务和系统是否正常运行。（提供产品截图） |
| 数据整合功能 | 可根据客户要求整合其他平台数据，如视频管理系统、环境监控系统等，统一在运维平台内展现。（提供产品截图） |
| 操作日志 | 系统应提供完整的软件操作日志审计功能，为管理者能清晰的查阅到对于资源设置变更、监控规则变更、报表规则变更的情况。 |
| 辅助值班配置功能 | 辅助值班功能作为独立模块集成到监控平台中，提供灵活的值班排定（按照周末和非周末、按日历等）、打印、值班短信提醒功能。监测的指标产生报警通过辅助值班配置向值班人员发送短信或者语音报警信息。（提供产品截图） |
| 系统自诊断 | 系统的自诊断性良好，在系统运行出现问题时系统会自动发生故障报警时间，以便及时通知值班人员解除现场故障。系统运行正常时报平安功能。 |
| 售后服务 | 提供原厂工程师本地化4小时到现场服务一年，负责系统的安装、测试、培训。并且做到一年4次的巡检服务，提供原厂承诺函并包含服务要求条款。 |
| 原厂商高级工程师上门安装、实施、培训。 |

2、内网110个用户杀毒软件一套

|  |  |
| --- | --- |
| 配置要求 | 1. 1个管理中心； 2. 服务器和工作站端共110并发用户(不分服务器和工作站)； 3. 管控中心安装授权无限制，支持对所有不同系统平台客户端进行统一管理，授权1年有效期内免费反病毒库及版本升级，授权1年有效期内免费售后支持服务。 |
| 安装部署 | 1.  支持常见的32位和64位操作系统：Windows XP Professional SP3、Windows Vista SP2、Windows 7 Professional、Windows 8 Professional、Windows Server 2003、Windows Server 2008、Windows Server 2012、Linux、Unix等。 2.可以通过产品部署安装包进行对全网现有反病毒软件进行统一自动卸载操作。 3. 支持多种安装方式，至少包括下载安装、远程安装、共享安装、Web安装、脚本登录安装和域组策略安装，支持通过管理控制台方式进行远程安装，支持通过WEB方式进行远程安装，支持局域网未安装用户的强制推送安装。 4. 客户端需提供软件防止配置随意修改保护功能、防止非管理员主动退出程序功能、反卸载功能（密码保护）及防止随意删除授权功能。 5. 要求产品集成病毒监控、防火墙、邮件反病毒、主动防御、入侵检测系统、网页反病毒、应用程序控制、设备控制、网页控制、漏洞检测和网络流量监控于一体。 6.  授权文件支持自动下发机制。管理服务器将自动收集网络中尚未激活或授权过期的计算机进行授权信息的下发。 7.客户端与服务器端可自动检测是否最新病毒库，支持手动和自动离线病毒库更新，支持强制推送更新。 8. 通过激活码或授权文件的形式来管理当前网络中的反病毒客户端授权。 9. 支持卸载第三方不兼容软件，可以扫描网络中其它的软件或不兼容的软件并进行卸载。 10.  可根据需求为反病毒程序或其他第三方应用程序创建定制化安装脚本。11．支持准入安装，只有允许的用户才能下载安装软件和更新。 |
| 病毒处理能力和防范能力 | 1. 能够实时监控和清除来自各种途径的病毒、木马、广告软件、恶意插件、隐蔽软件、黑客工具、风险程序等。 2. 对各种常用压缩格式文档中的病毒能有效的进行实时检测和处理，并能对任意层数压缩文档进行扫描操作（至少20层以上）。支持2000 种以上存档和压缩格式的扫描，可以对rar、zip、cab、arj等压缩格式的病毒做到包内清除。 3. 可以隔离被感染的计算机。如果网络中的一个工作站被感染，程序会在一段时间内阻止用户访问服务器资源。 4. 发现病毒后，有多种处理方法，例如清除、删除或隔离（隔离区可进行自定义），所有方法可在管理控制中心统一设置以及在客户端单独设置。 5. 具有未知病毒检测、清除能力，支持变种病毒的查杀，能够对各种加壳的病毒文件进行病毒查杀。 6.反病毒软件需要具备个人防火墙功能,有效对存储在计算机中的个人数据进行保护，阻止所有通过本地网络或互联网进行计算机的各种威胁。 7.反病毒软件需要具备IDS/IPS功能，以及病毒爆发监控和入侵行为检测功能，一旦客户机连接异常，可以迅速发出报警或隔离被感染的计算机。 8. 可以主动防御威胁。例如，危险行为，隐藏进程（rootkits），Windows系统钩子，键盘记录器等，让用户的上网更加放心。 9. 工作站端在处理病毒后可逆向操作，如有对病毒做删除处理的动作须在删除前对文件进行备份，以便以后可进行还原恢复操作。 10. 具备自动识别新建的和被修改的文件的能力，并且可以定义扫描文件范围。 11. 反病毒软件可以通过邮件协议和邮件终端内嵌两种方式进行邮件的实时病毒监控。最少支持对以下三种协议和两种客户端POP3/SMTP/IMAP/NNTP，The Bat!/ Microsoft Office Outlook/Foxmail/Outlook Express。 12. 即时通讯工具防护，支持对MSN、ICQ、QQ、SKYPE等中最少两种进行URL过滤和文件扫描等。 13. 反病毒软件需要具备启发式扫描技术，并且可以对打开文件、运行进程、静态文件等进行未知威胁检查，并且对于通过HTTP、FTP、SMTP、POP3等常用协议的数据流进行未知威胁扫描。 14. 能够进行内存查毒，清毒。 15. 能够对运行文件进行清毒。 16. 反病毒软件能够自动隔离被感染且暂时无法修复的文件，并在用户许可的情况下传送至生产商。 17. 支持IPv6和无线网络的管理。 18. 产品具备有效抵御各种最新威胁的机制和功能，可以更加快速的对最新恶意程序进行响应。 |
| 管理控制 | 1.     有良好的可扩展性和易用性，支持大型网络跨地域、跨网段的部署和管理，支持VPN的MMC管理，支持无限层网络架构，支持C/S及B/S两种模式对客户端进行管理。 2.     管理控制中心能对所有客户端进行集中的管理和远程控制，可以通过控制台直接给客户端发送命令，诸如强制客户端启动、停止、立即杀毒、立即升级、定时杀毒和升级等，采用国际标准的SSL加密方式。 3.     管理控制中心能够实时显示客户端的状态，当客户端查杀到病毒时，能够实时将病毒信息以报告的形式上报给控制台。 4.     支持分组和分级管理，对任意策略都具备分组、分级授权功能。 5.     具有病毒日志查询与统计功能，可以随时对网络中病毒发生的情况进行查询统计，统计显示饼状图、柱状图等，能按时间（日、周或任意时间段）、按IP地址、机器名、按病毒名称、病毒类型进行统计查询，能将查询统计结果打印或导出，导出支持多种格式。 6.     管理控制中心具备智能分担因数据库更新下发所产生的网络负载，节省整体网络资源（具有网络更新代理服务器设置功能，智能分担管理控制中心数据库集中发布整体负载，节省企业网络资源）。 7.     管理控制中心可以对所提供的不同系统平台以及应用系统下的防护终端进行统一控制。 8.     管理员可锁定客户端的使用权限。当客户端开机时，可以运行错过的计划任务。 9.      管理控制中心支持向客户端发送广播消息。10.   能够在管理控制中心上向多个目标系统分发新版安全产品，并说明分发方式。 11.   自动扫描网络中不被保护的计算机（IP 子网/活动目录/工作组），确保全网机器安全运行与部署。 12.  具有减少网络负载功能，管理控制中心可针对IP子网或者IP段进行数据传输速度的控制；通过建立相关配置规则，可对最大传输速率和时间等参数进行定义。 13.  在管理控制中心，可以远程连接到客户端计算机来体验并解决问题；如：获取系统信息，运行的程序，针对不同的进程提取日志文件，必要时运行某些工具等。 14.   管理控制中心可将全网客户端隔离区中、备份区文件拷贝到管理控制中心并进行统一处理。 15.  管理控制中心需要可以与Network Access Protection (NAP)协议进行互动，对于网络中的客户端信息进行有效的收集。 16.  管理控制中心需要支持对于反病毒数据库的更新后自我验证功能，确保对于全网客户端计算机反病毒数据库更新的有效性。 17.  管理控制中心可以通过自身功能对全网客户端中安装的第三方应用程序信息进行收集，并且可以进行信息分类操作。 18.  管理控制中心需要具备提供多种对于网络中计算机查找机制，包括IP、IP段、系统信息、计算机感染病毒情况、安装防病毒程序等。 19.  管理控制中心需要具备通过标准的SNMP协议进行全网监控和管理的功能。 20.  管理控制中心需要能够收集网络中被管理客户端硬件情况的详细信息。 21.  管理控制中心能够统一对全网客户端中应用程序启动和运行权限进行统一管理。 22.  管理控制中心能够统一对全网客户端中外接设备的读写权限进行统一管理。 23.  管理控制中心能够统一对全网客户端中网页访问权限进行统一管理。 24.  要求管理控制中心能够检测统计网络中被管理客户端的操作系统及所安装系统软件的漏洞信息，并支持客户端漏洞补丁的下载和安装，支持手动、自动及强制推送。 25.  管理控制中心需要能够支持内部云建设，减少网络负载。 26.  客户端反病毒软件中云技术的开启或关闭必须能够由管理控制中心集中管理。 27.  能够支持在不增加硬件设备的情况下实现管理控制中心分级管理。 28.   管理控制中心支持支持Windows故障转移集群，提供高可用性并增强服务器的稳定性。 29.   管理控制中心支持自动备份管理服务器数据，防止反病毒系统状态和设置的关键数据丢失。 30.  管理控制中心需要能够统计客户端被禁用的外接设备的连接情况，并允许客户端临时使用外接设备。 31.  可以通过管理中心对客户端进行所有加密相关的设置和策略的制定。 32.  可以对不同客户端中磁盘进行加密操作，并且可以设置排除磁盘加密。 33.  可以对指定文件和文件夹进行加密操作，包括：自定义文件夹、文件扩展名、预定义文件夹、应用程序产生文件和自定义分组。 34.  可对移动存储设备进行整盘、文件和便携式加密存储器操作。 35.  可以通过管理中心对目标计算机系统进行镜像提取，提取后不改变系统和已安装应用程序。 36.  可以通过管理中心对未安装系统目标计算机推送系统镜像。 37.  管理控制中心可建立内网WSUS服务器，为内部终端系统进行补丁下载和安装。 38.  管理控制中心可以对企业网络内应用程序进行授权管理，并能够根据应用程序名称、制作厂商和版本进行条件定义。 39.  管理控制中心对企业网络内部可进行准入控制管理，对IP、Mac地址、子网和IP地址范围进行计算机定义，对计算机状态、制造商、域成员关系、企业设备和软件进行定义。 40.  管理控制中心可以对客户端进行应用程序自动安装操作，并且管理员可以自定义选择需要安装的应用程序。 41.  管理控制中心可以包括恶意程序防护、加密、系统补丁、系统镜像、网络准入控制在内的所有组件进行统一管理。 |
| 升级更新 | 1.在服务期内，提供免费的反病毒库更新和产品升级信息服务。 2. 反病毒软件在更新过程中遇不可抗力等意外情况下中断，在下次重新运行更新时，可使用增量更新技术，在中断之前更新的基础上继续更新，提高更新效率，节约网络流量。 3. 反病毒软件需拥有回滚反病毒数据库功能。在遇到不可抗力等意外情况下，反病毒数据库损坏时，可以成功恢复上一次完成更新时的状态，保证反病毒软件正常运作。 4. 防病毒软件的控制台更新后，能够有效、及时、自动地完成全网反病毒客户端的更新。 5. 支持客户端通过Internet升级，使客户端在连接不到控制中心的情况下，能够通过互联网进行升级，不另外收取费用。 6. 要求有快速的反应能力，反病毒数据数据库要求常规平均每个小时更新一次，反病毒更新模块允许从 Internet 或当地的服务器下载最新的反病毒数据库和组件。 |
| 产品培训、支持服务 | 1.免费提供计算机病毒防治技术咨询与产品技术支持服务；服务方式可通过电话、电子邮件、传真、现场服务等。 2. 为用户提供公开的400或800免费电话，获得5 \* 8小时的技术服务，电话号码可在投标产品生产商的官方网站上查询。 3. 提供本地产品售后电话回访，及授权的认证工程师上门服务；在接到用户求助后，1小时内做出响应，4小时内到达现场，24小时内处理和解决问题。 4.对提交的可疑文件（包括新病毒），厂商必须在接到可疑文件的24小时内给予答复。 |

3、机房IT设备硬件运维

包括对全局范围内所有IBM服务器（4台）、联想服务器（1台）、戴尔服务器（2台）等设备的运维。具体包括但不限于统计、登记、盘剥、清灰、清洗，管理、检查、维护、维修、更换，配置、调整、优化、升级、加固，监控、测试、预警、报警、排障，应急等工作（包含硬件故障维修更换的费用）。保障设备正常的运行。

4、软件维护工作

服务器监控软件、SQL server、Oracle、操作系统等软件平台的运维及漏扫安全防护，并对系统及杀毒应用软件的日常维护升级提供支持。对第三方的系统升级提供协助服务。

5、配套设施及其他服务

除了上述服务外，还需提供其他服务，包括：服务支持、专业巡检服务、软件版本升级服务、专项服务、数据备份、数据容灾、数据恢复、系统恢复、培训服务、文档制作、UPS测试、应急演练、安全测评、软件漏洞打补丁、软件升级、软硬件加固、网站安全监控等。

特别注意：

本项目包含软硬件系统安全服务费用，硬件故障更换、维修费用及合同有效期内增加的设备维保费用，包括应急演练、备份、容灾、数据恢复、系统恢复等所涉及的所有费用都包含在此次招标费用内，招标方不另支出相关费用。

要求2次所有服务器除尘服务；每年2次信息安全检查整改并出具书面材料每年2次全系统操作或安全培训，每年1次信息中心技术人员技能提升培训，每年2次系统级应急演练，每年2次数据恢复容灾演练。保障各系统正常运转。

二、维护方式

1、人员构成：

服务方提供3名专业的技术工程师现场进行运维服务：

1名高级工程师熟悉主流网络架构、安全设备、服务器、GIS等设备及系统的运维，熟悉省市电子政务网、涉密网、公安网、运营商网络，熟悉安全测评、等级保护及各级各类业务系统的部署，计算机相关专业毕业，本科及以上学历；

2名网络工程师日常上门服务设置AB岗，熟悉主流操作系统、系统软件，如Windows、Linux、Oracle、SQL server、杀毒防毒软件等，如有特殊情况，需按业主方要求，提供无条件额外服务。对各信息系统、机房等定期巡检、应急演练、安全测评、业务培训等。工程师服从业主方统一安排，工作时间、工作任务由业主方分配，要遵守业主方的规章制度，如有违反，将以扣款处理。甲方提出需要驻场人员时，技术人员需无条件响应。如乙方需要服务凭证，甲方需提供书面凭证。如服务人员多次违反规定，或不能满足业主方要求的，业主方有权要求中标单位更换人员。中标单位还要加强服务人员的保密、安全责任等方面的管理工作。当中标单位如要更换服务人员，需提前一个月通知业主方，做好工作交接。

2、技术支撑：

设备或系统出现故障时，需提供24小时不间断维护，监控软件辅助与人工巡查结合。要求投标人接到采购人服务电话后1小时到达现场，系统或软件故障4小时之内解决问题；若硬件设备故障无法在4小时内解决的，需要提供相应备件，备件技术性能须满足项目需要，备品备件清单内的设备，2小时内提供备机，其他设备24小时内提供备机。

三．服务人员要求

|  |  |  |
| --- | --- | --- |
| 人员名称 | 职责及要求 | 数量 |
| 高级工程师1名 | 熟悉主流网络架构、网络设备、安全设备、服务器、存储、容灾备份、网管软件、UPS、精密空调、环境监控等设备及系统的网络运维，须具备CCNP及其他网络同等认证证书，并具备本科及以上学历。要求有3年以上政府机关机房维保经验，要求无判刑、刑拘等不良记录，工作勤勉、踏实、细心、负责，熟悉《浙江省电子政务网络技术规范》、《浙江省电子政务网络安全规范》。 | 1 |
| 系统运维人员2名 | 熟悉主流操作系统、常用系统应用软件、如Windows、Linux、Oracle、Sybase、SQL server、office、杀毒防毒软件等软件部署实施维护等。服务器及存储安全设备的日常硬盘排错更换等服务。其中1人须具备微软产品认证资质。2年以上专业的技术服务经验，要求无判刑、刑拘等不良记录，工作勤勉、踏实、细心、负责，熟悉《浙江省电子政务网络技术规范》、《浙江省电子政务网络安全规范》。配置2人做AB岗位。 | 2 |

四、违约责任：

中标单位应当履行合同约定的义务，如有违反，须承担相应的违约责任，未满足标书要求或承诺但不能兑现的，除承担违约责任外，需赔偿相关损失：

1．响应不及时。未在规定时间内提供服务及要求履行的事务时，每次罚1000元。

2．维护、检修、升级服务不到位。每次罚500元至1000元不等。

3. 如在合同规定的维保期内，达不到项目规定的技术指标、业主要求，中标单位应当承担违约责任。承担方式和违约金额如下：超期10天内，每天扣合同金额的0.1%；累计超期10天，甲方有权终止执行合同。

4. 因中标单位原因造成业主系统不能正常运行，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，赔偿金额为项目总价的10%。

5. 服务过程中，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，风险责任由中标单位全部承担。

6. 甲方提出跟换工程师，投标人需一个月内响应，如不予响应，超过一个月以上的，每天扣款200元。

**第四部分 评标办法**

本次评标采用综合评分法，总分为100分，其中价格分20分，技术分75分，资信及其他分5分共三部分。合格投标人的评标得分为各项目汇总得分，中标候选资格按评标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，按技术得分由高到低顺序排列。排名第一、第二的的投标人为中标候选单位。评分过程中采用四舍五入法，并保留小数2位。

投标人评标综合得分=价格分+技术分+资信及其他分。

|  |  |  |
| --- | --- | --- |
| 评分项目 | 评分要点及分值 | 说明 |
| 价格(20分) | 采用低价优先法（0-20） | 满足招标文件要求且投标价格最低的投标报价为评分基准价，其他投标人的价格分按照下列公式计算：报价得分＝（评标基准价/投标报价）×20×100%。投标人的投标报价超过预算金额，将作为无效标。 |
|
| 技术方案及质量（75分） | 对业主单位基本现状的理解与表述（0-8分） | 1、对采购人组织架构、业务系统、流程、制度熟悉情况（0－4分）；2、投标人对采购人硬件设备状况及所涉及的软件平台等其他资源、环境的熟悉程度，能准确掌握采购单位设备现状、网络整体部署情况以及维保设备具体配置情况和使用情况的（0－4分）； |
| 详细项目实施及技术解决方案(0-17分) | 1、提供的维护维保服务方案（内容）是否满足采购人的要求，在同等级服务中是否具有优势，完全符合招标文件技术指标要求的得10分，非关键参数有负偏离或缺漏项的每项扣3分，扣完为止（0－10分）；2、运维实施方案（定期巡检、监测、优化、培训、重大活动、节假日保障等）（0－5分）；3、运维质量管理和流程规范程度（管理制度、流程图、记录、表单）（0-2分）； |
| 运维监控软及杀毒软件（0-10分） | 运维监控软件要求符合招标文件里的内容(包含证书、截图、厂商质保等)（0-7分）；杀毒软件要求符合招标文件里的内容(包含证书、截图、厂商质保等)（0-3分） |
| 维护维保服务保障措施（0-13分） | 1、服务承诺的可行、完整以及服务承诺落实的保障措施得力程度（0－2分），2、服务器监控软件提供原厂商技术支持和售后保障证明材料；最高6分（0－6分）；4、运维服务的响应时间、故障解决问题的速度和方式，流程设计的横向对比（0-5分）； |
| 应急保障措施（0-5分） | 应急预案及备份方案的可行性与完整性（0-5分）。 |
| 备品备件保障情况（0－3分） | 对采购人的系统设备的配件、附件、备品备件的准备和保障措施情况，在杭州市区设有的备品备件库情况，特别是关键部件的设备的完备情况，是否能提供快速的服务响应，确保采购人系统设备正常运行（0－3分）。 |
| 优惠和承诺（0-3分） | 投标人提出的对本项目的实质性优惠条件和承诺情况，承诺满足招标文件要求得2分，提供其他实质性优惠承诺的酌情得分，最高加3分。 |
| 维护工程师配备情况（0-10分） | 服务工程师中有具备IBM、DELL、联想服务器厂家认证证书的得5分，具备微软、oracle认证证书得3分，具有政府机关3年以上机房服务经验得2分。认证证书复印件，证书原件备查。此项最高得10分。 |
| 项目组人员素质情况（0-6分） | 运维项目组成人员数量、职业资格、团队维保能力情况，提供的本项目组服务人员相关服务经验介绍、从业时间及所在投标单位任职时间等（提供相关资格证书和服务经验、业绩）。项目组成员具有项目经理证书得1分，具有高级项目经理证书得2分，最高2分；项目组成员具备IBM、戴尔、杀毒软件等安全厂商认证工程师；每项得2分；最高4分 |
| 商务资信分（5分） | 投标人业绩情况（0-3分） | 投标人近三年来（以合同签订日期为准）浙江省及杭州市政府单位案例每项得1分；此项综合最高得3分。（原件待查）(0-3分)。 |
| 投标书编制质量(0-2分) | 根据投标文件编制是否完整有序、装订整齐、书面整洁、内容详实，内容无前后矛盾，符合招标文件要求等评分。(0-2分)。 |