安徽文达信息工程学院

招

标

文

件

项目名称：服务器及客户机杀毒软件

采购单位：安徽文达信息工程学院

日　期：2019 年 3 月 25 日

招标公告

一、项目名称：

1、项目名称：服务器及客户机杀毒软件

2、项目地点：实资处（信息技术中心）

3、项目单位：实资处（信息技术中心）

4、项目概况：见参数

5、资金来源：自筹

6、项目类别：货物

二、投标人资格及要求：

1、投标人须符合《中华人民共和国政府采购法》的规定条件；

2、注册于中华人民共和国境内，具有独立承担民事责任的法人或其他组织；

3、具有良好的商业信誉和健全的财务会计制度，经营活动中没有违法记录；

4、投标人具有独立法人资格，有能力提供该货物及服务的国内代理商或制造商，具有有效的营业执照、组织机构代码证、税务登记证（三证合一的可仅提供营业执照）注册资金不少于 200 万元；

5、若为代理商投标，则需提供制造商为其出具的授权书原件,扫描件、复印件无效；

6、、企业（供应商或制造商）必须提供近三年（2016 年 1 月 1 日至今）在安徽省内高校同类型产品三份以上供货合同；

7、本项目不接受联合体投标；

8、具有履行合同所必需的设备和专业技术能力；

9、所有提供的设备应具备完善的售后服务保障承诺和服务年限。

三、投标人提交资料：

1、提供（营业执照、税务登记证、组织机构代码证或三证合一）副本加盖公章的复印件；

2、个人身份证（加盖单位公章的复印件）；

3、法定代表人授权委托书（原件）。

四、报名时间、地点及方式：

1、报名时间：2019年3月25日到开标前3小时止；

2、招标文件价格：300元；

3、报名方式： （1）现场报名，（2）也可转帐购买文件，通过邮件发送营业证照；

4、报名地址：安徽文达信息工程学院后勤集团采购中心。

五、开标时间：另行通知。

六、采购项目联系人及电话：

联系人：杨老师 电话：18956035539 曹老师 18788882459

投标人须知前附表

序号	内容	说明与要求
1	采购人	安徽文达信息工程学院
2	项目名称	服务器及客户机杀毒软件
3	项目性质	货物类
4	资金来源	采购人自筹
5	付款方式	付款方式：货物验收合格后在 2019 年 9 月份付总货款的 60%,合同签订壹年付到总货款的 95%，质保贰年到期后付清余款。
6	供货地点	安徽文达信息工程学院
7	勘察现场	自行勘察
8	投标文件份数及要求	正本 1 份；副本 4 份密封提交
9	开标时间及地点	开标时间：另行通知 开标地点：安徽文达信息工程学院振宁楼一楼后勤会议室。
10	评标办法	议标（竞争性谈判） 一、使用单位提供安徽省内三所以上已使用同类型产品的高校，招标小组组织做好前期调研工作； 二、投标单位必须提供三份以上同类型产品的供货合同； 三、中标结果以我校发布的中标公告为准。
11	报价货币币种形式	本项统一采用人民币报价

投标人须知

一、适用范围

本招标文件仅适用于本次招标所述的货物项目采购。

二、有关定义

1、采购人：系指本次采购项目的业主方。

2、投标人：系指按规定获取了本招标文件，且已经提交或准备提交本次投标文件的制造商、供应商或服务商。

3、货物：系指各种形态和种类的物品，包括原材料、燃料、设备、产品等，包括与之相关的备品备件、工具、手册及安装、调试、技术协助、校准、培训、售后服务等。

本招标文件所采购的货物、产品、配件等全部标的，均应是全新、未使用过的，是完全符合相应质量标准的原装正品。无论招标文件是否列明，投标人所提供的货物、产品、配件均须符合国家产品质量、安全、卫生、环保、检疫检验、生产经营许可等现行法律法规的规定，且在投标时已具备，否则投标无效。本招标文件所要求的证书、认证、资质，均应当是有权机构颁发，且在有效期内的。

4、近 X 年内：系指从开标之日向前追溯 X 年（“X”为“一”及以后整数）起算。除非本招标文件另有规定，否则均以合同签订之日为追溯结点。

5、业绩：系指符合本招标文件规定且已供货（安装）完毕的与最终用户(“最终用户”系指合同项目的建设方或由建设方确定的承包方)签订的合同及招标文件要求的相关证明。投标人与其关联公司（如母公司、控股公司、参股公司、分公司、子公司、同一法定代表人的公司等）之间签订的合同，均不予认可。

三.投标费用

无论投标结果如何，投标人应自行承担其编制与递交投标文件所涉及的一切费用。

四.合格的投标人

1、合格的投标人应符合招标文件载明的投标资格。

2、除非招标文件认可，否则母、子公司之间的业绩、资质不得互用。

3、投标人之间如果存在下列情形之一的，不得同时参加同一标段（包别）或者不分标段（包别）的同一项目投标：

4、法定代表人为同一个人的两个及两个以上法人；

5、母公司、全资子公司及其控股公司；

6、参加投标的其他组织之间存在特殊的利害关系的；

7、法律和行政法规规定的其他情形。

五.报价

1、**投标人应按本招标文件内所有项目的单价报价**（免费赠送的除外），并合计总价。

2、投标人的报价应包含所投货物、保险、税费、包装、加工及加工损耗、运输、现场落地、安装及安装损耗、调试、检测验收和交付后约定期限内免费维保等工作所发生的一切应有费用。

3、报价应当低于同类货物和服务的市场平均价格。

4、采购人不建议投标人采用总价优惠或以总价百分比优惠的方式进行投标报价，其优惠可直接计算并体现在各项投标报价的单价中。

5、 除非招标文件另有规定，报价一般按精确到小数点后两位计算。

6、除政策性文件规定以外，投标人所报价格在合同实施期间不因市场变化因素而变动。

7 、对于进口产品的报价，投标人应报出CIP合肥的价格。本项目进口产品统一采用人民币报价。

六.勘察现场

1、投标人应自行对供货现场和周围环境进行勘察，以获取编制投标文件和签署合同所需的资料。勘察现场的方式、地址及联系方式见投标人须知前附表。

2、勘察现场所发生的费用由投标人自行承担。采购人向投标人提供的有关供货现场的资料和数据，是采购人现有的能使投标人利用的资料。采购人对投标人由此而做出的推论、理解和结论概不负责。投标人未到供货现场实地踏勘的，中标后签订合同时和履约过程中，不得以不完全了解现场情况为由，提出任何形式的增加合同价款或索赔的要求。

3、除非有特殊要求，招标文件不单独提供供货使用地的自然环境、气候条件、公用设施等情况，投标人被视为熟悉上述与履行合同有关的一切情况。

七.知识产权

1、投标人须保证，采购人在中华人民共和国境内使用投标货物、资料、技术、服务或其任何一部分时，享有不受限制的无偿使用权，不会产生因第三方提出侵犯其专利权、商标权或其它知识产权而引起的法律或经济纠纷。如投标人不拥有相应的知识产权，则在投标报价中必须包括合法获取该知识产权的一切相关费用。如因此导致采购人损失的，投标人须承担全部赔偿责任。

2、投标人如欲在项目实施过程中采用自有知识成果，须在投标文件中声明，并提供相关知识产权证明文件。使用该知识成果后，投标人须提供开发接口和开发手册等技术文档。

八.纪律与保密

1、投标人的投标行为应遵守中国的有关法律、法规和规章；

2、投标人不得相互串通投标报价，不得妨碍其他投标人的公平竞争，不得损害采购人或其他投标人的合法权益，投标人不得以向采购人、评标委员会成员行贿或者采取其他不正当手段谋取中标；

3、供应商直接或者间接从采购人处获得其他供应商的相关情况并修改其投标文件或者响应文件；

项目四：服务器杀毒软件采购

杀毒软件参数要求

数量：十五(套)盒装，存储介质印有正版序列号

质保期：三年

技术指标		指标要求
环境要求	控制中心安装环境要求	操作系统支持 Windows Server 2003/2008 R2/2012/2012 R2/2016 的 32 位和 64 位版本（简体中文版）； ★支持 Cent 0S 7、Redhat 7 等 Linux（要求 docker 版本务必大于 1.8.2）
		支持在虚拟机上安装控制中心
系统管理		控制中心：具备设备分组管理、策略制定下发、全网健康状态监测、统一杀毒、统一漏洞修复、网络流量管理、终端软件管理、硬件资产管理以及各种报表和查询等功能；
		客户端提供控制中心管理所需的相关数据信息，通讯可选择非明文方式；客户端执行最终的木马病毒查杀、漏洞修复等安全操作；
		产品支持终端保护密码，设置密码后，终端退出或卸载杀毒、或安装控制中心，都需要输入正确的密码方可执行；要求客户端程序具备自保功能，避免被恶意篡改
		支持网页访问部署、离线安装包部署、域推送等部署方式，可自定义部署通知邮件及部署通知公告；
		支持自定义默认分组的终端默认功能模块，包括产品功能模块及实用工具等；
		支持加密的控制中心远程访问，支持管理账户并发、密码有效期、鉴别失败锁定等设置；支持设置日志上报的带宽限制；
		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；
		支持控制中心迁移、数据备份、数据恢复；支持多升级服务器；
日志报表		展示全网终端健康状态、报警信息；可方便的查看不健康、亚健康终端列表；展示全网终端病毒库日期比例，可方便的查看全网终端病毒库的情况。
		展示指定时间内指定终端修复漏洞，病毒查杀，木马查杀的情况；
		要求支持邮件报警，可以设定多种触发条件，满足条件后自动发送邮件到相关人。邮件触发条件至少包括：一定时间内的病毒数量阈值、一定时间内的未知文件数量阈值、重点关注的终端发现病毒、病毒库超期等；
		提供系统升级、热备、管理员操作、管理员远程等系统日志；
	内存防护	支持内训实时监控查毒，能够自动隔离感染而暂时无法修复的文件；
	启动防护	支持抢先加载病毒，在系统未加载前启动文件监控，通常情况下不必重启到安全模式也能清除病毒；
	注册表、引导区防护	支持文件、引导区、内存、注册表、服务、进程、进出文件、目录、压缩文件、网页等恶意代码、恶意样本查杀；
	电子邮件防护	支持电子邮件内文件检测，可清除隐藏于电子邮件计算机病毒和恶性程序；
	网页安	能够对网页提供安全防护，发现网页中的危险行为实时阻断；能够对网页

病毒、恶意代码、木马防护	全防护	额木马进行拦截，能够自动拦截网页中的钓鱼、欺诈信息；
	网络安全防护	拦截下载器自动下载木马程序、恶意推广程序、盗号木马；拦截黑客远程控制本机；
	嵌入式防御	支持用户添加嵌入杀毒的应用程序；支持 FlashGet、NetAnts、WinZip、WellGet、WinRAR 等工具的嵌入式杀毒功能；
	移动设备病毒防护	要求提供 U 盘等移动设备接入电脑自动检测功能，全面拦截和清除在移动设备接入系统可能带来的病毒木马；
	局域网共享查杀	能够对局域网共存文件传输进行检测和查杀；
	浏览器防护	支持浏览器防护，对篡改浏览器设置的恶意行为进行有效防御，并可以锁定默认浏览器设置；
	聊天安全防护	检测相关常用聊天软件传输文件的安全性，确保传输文件不中毒；检测聊天软件中对方发来网址的安全性 ★聊天 软件传输某些文件会添加“.重命名”，如果文件安全，将自动去除“.重命名”；
	输入法防护	要求可以拦截伪装输入法程序的木马； 要求拦截利用输入法启动的木马程序；
	文件传输防护	支持 U 盘等移动磁盘设备和电脑硬件间文件传输检测； 支持局域网共享文件传输检测；
	攻击防护	能够实时检测和拦截攻击行为，包括改写系统关键文件、修改注册表关键键值、感染移动村塾截止、创建系统账号；
	★云修复	支持扫描发现文件遭破坏或被感染时触发修复流程，修复通过公有云下载正常文件替换遭破坏的文件；
	定时查杀	要求能够自定义时间、自定义扫描频率，自定义扫描类型，对终端进行定时查毒，并且可以自定义查杀病毒后的处理方式自定义；
	黑白名单例外	支持文件、目录和数字签名自定义黑白名单的方式来管理全网终端的文件； ★支持手工导入 MD5+SHA1 的黑白名单方式，支持 txt 批量导入方式；文件被加入白名单，客户端不在查杀，加入黑名单，客户端不可执行此文件； ★支持下发忽略白名单的病毒扫描； ★支持对 Windows/Linux 操作系统终端的文件黑白名单和信任区在服务端统一管理；
	病毒查杀统计	要求支持通过数字签名或者文件名的方式分别显示文件，方便管理员管理全网终端上报的文件；
		支持按病毒、木马、终端等维度统计全网病毒感染状况；
		要求支持对网内未知文件云查询的控制，可以选择直接连接互联网云查询中心查询，也可以选择采用私有云查杀引擎完成未知文件查询；
		要求上报文件至少包括：文件名称、发现时间、鉴定结果、文件大小、数字签名和文件所属源计算机等信息；
	压缩包杀毒	要求支持文件解压缩病毒查杀，支持对 Zip、RAR、7Z 等多种格式的压缩文件查杀能力；
	备份区隔离区管理	可对备份区、隔离区的文件进行有效管理；能够对单个、指定的文件和全部文件进行文件的删除、恢复等多项管理措施；

	多杀毒引擎	要求产品具备本地多引擎查杀能力，且引擎可配置；
	云桌面杀毒	★支持云桌面产品杀毒
	私有云引擎	要求产品具备公有云于本地私有云检测能力；
		支持部署私有云查杀引擎，增强本地隔离网查杀效果；
	病毒库升级	要求支持服务器端病毒库的定时更新和手动更新两种升级模式；
		要求支持客户端升级时对网络带宽的保护，可以设定服务器端最大升级带宽
补丁分发与漏洞修复		要求产品具有定时修复漏洞功能，同时可以设置筛选高危漏洞、软件更新、功能性补丁等修复类型；
		支持漏洞修复影响文档时提醒功能；
		支持补丁下载安装顺序设置，可以有效节省漏洞修复时间与减少 CPU 占用；
		支持自定义补丁排除名单，防止终端打补丁后造成系统或业务进程崩溃；
		★支持设置对特定分组有限进行补丁分发，一段时间后再全网升级；
		★终端支持智能屏蔽过期补丁与操作系统不兼容的补丁，可以查看或搜索系统已安装的全部补丁
		★产品具备漏洞集中修复，强制修复，自动修复，具备蓝屏修复功能；
		要求产品生产公司具备热补丁修复功能
		★产品具备漏洞集中修复过程中的流量控制和保证带宽，补丁分发支持服务器端带宽限流与客户端 P2P 补丁分发加速，有效节省外网带宽资源；
运维管控		★支持远程协助终端（不依赖 Windows 远程桌面协议）、远程关机、重启终端；支持远程操作时锁定屏幕、截取屏幕，远程锁定屏幕后需要输入解锁密码才可再次使用；
		可监控指定终端网络、应用程序的上传，下载速度与流量；
		支持冗余有线网卡、无线网卡、3G 网卡、modem、ADSL、ISDN 等设备的外联控制；违规外联发生是可针对内外网连接状态分别设置违规处理措施；
		支持终端进程红名单、黑名单、白名单功能，可设置核心进程必须运行，也可保护核心进程不被结束；
		支持网址白名单，通过信任网址白名单可以管理企业网络内信任的网址，加入信任后终端不再将此网址视为威胁 支持网址黑名单，可设置终端不能方位的网址 URL，终端访问这些 URL 时会被拦截，并展示拦截记录
		支持对终端各种外设（USB 存储、硬盘、存储卡、光驱、打印机、扫描仪、摄像头、手机、平板灯）、接口设置使用权限
		支持对终端桌面系统的账号密码、本地安全策略、控制面板、屏保与壁纸、浏览器安全、杀毒软件检查；
		终端支持在线、离线策略，可同时使用在线或离线两种状态，保证终端安全运行；