**附件一**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **序号** | **名称** | **技术参数及要求** | **参数响应** | **备注** |
| **1** | 上网行为管理 | 1. 网络吞吐量≥20Gbps 、推荐带宽≥1.5Gbps、支持用户数≥10000、每秒新建数≥20000、最大并发数≥80万，内存≥8GB，硬盘容量≥900G minisata SSD， 至少具备6个千兆电口，2个万兆光口SFP+（含满配光模块），1个串口(RJ45)， 2个USB接口，交流冗余电源（220V）标准机架设备，具备基本流量审计、应用审计、行为审计等功能； 2. 支持网关、网桥、旁路模式部署；网关模式，支持NAT、路由转发、DHCP、GRE、OSPF等功能； 3. 支持部署在IPv6环境中，设备接口及部署模式均支持ipv6配置；所有核心功能（上网认证、应用控制、流量控制、内容审计、日志报表等）都支持IPv6；（需提供相关功能截图证明）； 4. 支持首页分析显示接入用户人数、终端类型、认证方式；带宽质量分析、实时流量排名；泄密风险、违规访问、共享上网等行为风险情况； 5. 基于“流量”、“流速”、“时长”设置配额，当配额耗尽后，将用户加入到指定的流控黑名单惩罚通道中（需提供相关功能截图证明）； 6. 支持通过抑制P2P的上行流量，来减缓P2P的下行流量，从而解决网络出口在做流控后仍然压力较大的问题（需提供相关功能截图证明）； 7. 在流量时长分析、用户行为分析、终端接入分析等纬度相关页面支持对统计结果的向下钻取查询； 8. 设备内置应用识别规则库，支持超过10000条应用规则数，支持超过6500种以上的应用，并保持每两个星期更新一次，保证应用识别的准确率； 9. 能够对新浪微博、腾讯微博、网易微博等进行细分控制，如：登录、浏览、发微博、上传附件等； 10. 厂商应是国家互联网应急中心（CNCERT）服务支撑单位（国家级），提供相关证明材料； 11. 要求提供上门安装调试及工程师3年7×24小时免费上门服务，提供原厂出具的针对本项目的授权书、服务承诺函，提供3年免费软硬件质保及3年URL规则库升级。并承诺在运维服务期间如出现网络安全事故，承担相应责任。 |  |  |
| **2** | 数据库审计 | 1. 最大纯数据库流量≥400Mb/s，数据库实例个数≥30个，SQL处理性能≥10000条SQL/s，日志检索性能≥500000条/秒。规格：内存大小≥8G，硬盘容量≥2T SATA，接口至少6千兆电口，标准机架设备； 2. 采用B/S管理方式，无需在被审计系统上安装任何代理；无需单独的数据中心，一台设备完成所有工作；提供图形用户界面，以简单、直观的方式完成策略配置、警报查询、攻击响应、集中管理等各种任务； 3. 支持主流数据库Oracle、SQL-Server、DB2、MySQL、Informix、Sybase、Postgresql、Cache、达梦、人大金仓、南大通用、MongDB、K-DB、（需提供相关功能截图证明）； 4. 支持对跨包SQL语句进行拼接，能够完整解析与审计超长SQL语句（超过1460字节），防止躲避审计的行为； 5. 数据库访问记录应至少包括发生时间、业务用户名、操作终端主机名及IP/MAC地址、终端工具名称、数据库名、表名、语句、返回结果等关键信息，可对日志进行细粒度解析、分类审计； 6. 设备必须自带默认策略(如黑/白名单、全审计、攻击特征等)，支持自定义策略和规则，方便用户灵活配置审计规则，支持以操作类型、时间、IP地址、用户名、主机名、终端名、数据库表、认证结果、敏感数据等作为事件识别规则。（需提供设备配置截图证明）； 7. ★单一设备可同时支持包括数据库审计、数据库防火墙、风险漏洞扫描、状态监控、敏感数据扫描等功能，能够按需扩展（需提供设备配置截图证明） 8. 厂商为国家信息安全漏洞共享平台CNVD技术组成员单位，提供CNVD官网截图证明或证书复印件； 9. 产品具有中国信息安全认证中心《中国国家信息安全产品认证证书》。 10. 要求提供上门安装调试及工程师3年7×24小时免费上门服务，提供原厂出具的针对本项目的授权书、服务承诺函，提供3年免费软硬件质保。并承诺在运维服务期间如出现网络安全事故，承担相应责任。 |  |  |
| **3** | 防火墙 | 1. 网络层吞吐量≥20Gbps，应用层吞吐量≥8Gbps，并发连接数≥220万，新建连接数（CPS）≥15万，SSL最大加密流量≥350M，IPSec VPN最大接入数≥1000，IPSec VPN≥加密速度400M。 至少具备6个千兆电口，2个万兆光口SFP+（含满配光模块），2个USB口和1个RJ45串口，交流冗余电源（220V），标准机架设备； 2. 产品采用自主知识产权的专用操作系统，应用多核并行处理技术保障产品处理性能，需提供公安部计算机信息系统安全产品质量监督检验中心、中国信息安全测评中心、中华人民共和国国家版权局、公安部信息安全产品检测中心之中任意一家检测机构出具关于“多核并行安全操作系统”的证书； 3. 支持链路健康检查功能，支持基于多种协议对链路可用性进行探测，探测协议至少包括DNS解析、ARP探测和PING方式； 4. 产品支持策略路由负载，支持基于服务、ISP地址、应用等维度进行智能选路，保证关键业务流量通过优质链路转发，支持加权流量、带宽比例、线路优先等负载均衡调度算法。（需提供相关功能截图证明）； 5. 产品支持僵尸主机检测功能，产品预定义特征库超过110万种，可识别主机的异常外联行为； 6. 产品支持管理员双因素认证功能，用户通过用户名/密码和Key等不同方式登陆产品管理界面； 7. ★产品支持勒索病毒检测与防御功能，为保障勒索病毒的防御效果，所投产品必须提供具备CMA（中国国家认证认可监督管理委员会）认证的第三方权威机构关于“勒索软件通信防护”功能项的产品检测报告； 8. 支持IPSec VPN智能选路功能，根据线路质量实现自动链路切换。（需提供产品功能截图证明）； 9. 厂商为国家信息安全漏洞共享平台CNVD技术组成员单位，提供CNVD官网截图证明或证书复印件； 10. 厂商应是国家互联网应急中心（CNCERT）服务支撑单位，提供相关证明材料。 11. 要求提供上门安装调试及工程师3年7×24小时免费上门服务，提供原厂出具的针对本项目的授权书、服务承诺函，提供3年免费软硬件质保、入侵检测、病毒库升级服务。并承诺在运维服务期间如出现网络安全事故，承担相应责任。 |  |  |
| **4** | web应用防护墙设备 | 1. 网络层吞吐量≥20Gbps，HTTP应用层吞吐量≥1Gbps，HTTP新建连接数≥150000，HTTP并发连接数≥2200000。规格：内存≥8G，硬盘容量≥128GB，接口至少6千兆电口+2万兆光口SFP+（含满配光模块），交流冗余电源（220V），标准机架设备； 2. ★产品采用多核并行处理架构，提供中国信息安全测评中心、公安部信息安全产品检测中心、中国软件评测中心、国家版权局之中任意一家机构出具的关于“多核并行安全操作系统”的证书或测试报告； 3. 支持虚拟网线部署、透明部署、路由部署、旁路镜像等多种部署方式，适应复杂使用环境的接入要求； 4. 支持识别HTTP异常，包含HTTP方法过滤、HTTP头部字段Referer、User-Agent等注入检测、Host检测、URL溢出检测、POST实体溢出检测、HTTP头部溢出检测、range字段防护、multipart头部字段异常检测、高危头部重复检测； 5. 支持超过6200种防护规则。其中Web应用防护规则超过4900种，Web应用漏洞攻击防护规则超过1300种。 6. 支持漏洞防扫描，包括404页面检测、WAF规则拦截频率检测、目录访问频率检测、使用不常见的HTTP请求方法、匹配强弱规则扫描、敏感文件扫描等扫描行为特征，支持自定义封锁扫描IP封锁时间、支持隐藏服务器信息（需提供相关功能截图证明）； 7. 产品原生支持BOT防护功能，可过滤机器人自动化流量，非联动其他组件或产品，并支持用户自定义URL保护范围和保护阈值。支持自定义开关获取访问者设备指纹信息（需提供相关功能截图证明）； 8. 支持通过被动扫描功能，业务系统进行黑链检测、Webshell检测、漏洞风险检测、配置风险检测、弱口令账户检测（需提供相关功能截图证明）； 9. 支持针对业务风险汇总，支持展示业务安全状态分布，包括已失陷业务、正在遭受攻击的业务、存在漏洞但暂时未被攻击的业务，以及最近7天内的漏洞风险分布情况； 10. 支持以安全策略模板方式快速部署安全策略，安全策略模板支持默认模板和自定义模板等多种格式； 11. 要求所投产品具备“Web应用防护系统”级别为EAL3+的信息技术产品安全测评证书,提供有效证书复印件； 12. ★厂商为国家信息安全漏洞共享平台CNVD技术组成员单位，提供CNVD官网截图证明或证书复印件。 |  |  |
| **5** | 日志审计 | 1. 默认包含主机审计许可证书数量≥50个，最大可扩展审计主机许可数≥100，可用存储量≥2TB，平均每秒处理日志数（eps）最大性能≥3500。规格：标准机架式，硬盘容量≥2T，接口至少6千兆电口； 2. 系统需全面支持IPv4/IPv6双栈协议，无需在被采集目标系统上安装任何软件；产品功能的实现无需额外增加服务器等设备，采用B/S架构操作方式，无需安装客户端软件； 3. ★设备支持聚合策略，可根据最大限定实际、最大集合次数、匹配规则配置策略聚合相应的原始日志产生安全事件，安全事件可自定义展示的字段内容，包括：事件类型、名称、级别、发生源IP地址、协议、开始时间、结束时间等，可查看事件详情和原始日志；（要求提供产品功能界面截图并加盖厂商公章证明）； 4. ★系统支持数据大屏展示攻击源和目的，可以集中展示安全事件类型、名称、事件等级等信息（要求提供产品功能截图）； 5. 支持基于时间切片进行事件统计的方法，并提供国家权威机构出具的证明文件； 6. 设备具备事件规则关联分析方法并提供国家权威结构出具的证明文件； 7. 设备支持基于因果式的状态关联分析和基于异常统计模型的检查分析功能，可挖掘不同类型、来源于不同设备或系统的日志或安全事件之间可能存在的关联关系，管理界面应提供关联规则设置功能； 8. 设备支持展示告警，支持告警确认，告警事件包含：事件级别、类型、策略、时间、状态等，可查看事件详情和事件溯源信息；（要求提供产品功能截图）； 9. 厂商具有国家计算机网络应急技术处理协调中心颁发的网络安全应急服务支撑单位证书 10. 产品具有《计算机信息系统安全专用产品销售许可证》，《IT产品信息安全认证证书 ISCCC》。 |  |  |
| **6** | 防病毒软件系统 | 客户端防护要求：  1、产品采用B/S架构，支持通过HTTPS方式登录管理控制台，管理控制台访问需进行加密访问；防病毒客户端支持Windows XP、win7/8 Embedded、 Windows 10等操作系统；提供100个客户端授权许可，配置主机防火墙、爆发阻止、Web站点信誉服务、预测机器学习、行为监控、勒索病毒防护功能模块。提供三年原厂免费病毒库升级服务。  2、支持主机入侵检测系统；防病毒软具备个人防火墙功能，有效阻止各种恶意威胁；支持针对终端根据基于源IP（支持IPv6）、目的IP（支持IPv6）、源端口、目的端口、应用程序及注册表项，出站、入站等进行安全配置。  3、★产品能够实时监控并清除来自各种途径的病毒、木马、蠕虫、恶意软件、勒索软件、黑客工具等恶意威胁；需提供多种扫描引擎不少于五种，针对于机器学习必须使用独立扫描引擎，同时所有防毒引擎必须为自主知识产品非OEM产品。（须提供系统功能截图证明）  4、对于文件扫描方式至少支持三种以上，包括所有文件统一措施、推荐扫描措施、以及针对不同类型病毒/恶意软件提供不同扫描措施，同时不同病毒/恶意软件类型不少于7种分类。  5、★支持拦截恶意URL功能，检测并阻止恶意的URL链接，并支持URL地址黑白名单功能；具备Web信誉评估功能，包含HTTPS通信扫描，结合云安全架构自动识别并屏蔽恶意站点，阻止病毒自动更新。（须提供系统功能截图证明）  6、★具备病毒爆发防御功能，当最新病毒爆发时，可在病毒代码未完成之前自动对网络中的病毒传播端口、共享等进行关闭，切断病毒传播途径，预防最新病毒的攻击。（须提供系统功能截图证明）  7、能够恢复由勒索软件威胁加密的文件，阻止与勒索软件关联的进程，并防止遭受危害的可执行文件感染网络；具备防勒索软件防护功能，管理界面提供配置项。  8、对非存储设备，如bluetooth、IEEE 1394接口、红外设备、调制解调器、PCMCIA卡等进行分项权限设置；可对插入移动存储引导区或者移动设备的所有文件进行扫描设置。  9、支持多种安装方式，至少包括下载安装、MSI程序打包安装、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。  10、客户端更新实现并发更新数量的控制，同时可以按不同时间段进行更新并发限制；  11、★资质要求：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》网络版防病毒产品（一级品）证书；生产厂商具备CMMI 5级认证证书；生产厂商具备中国电子工业标准化技术协会颁发的ITSS《信息技术服务标准符合性证书》（业务领域：运行维护服务，评估等级：三级）；  服务器防护要求：  1、★控制中心能够与虚拟化平台无缝对接，支持适配主流虚拟化平台，如Vmware、华为FusionSphere、华三CAS等（须提供官方兼容性列表或证明文件）；产品支持有代理和无代理模式部署，并能够实现同一个控制中心管理；本次采用有代理部署模式，提供100个服务器授权许可，配置防病毒、Web信誉检测、功能模块。  2、提供AV防病毒，防恶意程序功能；提供Web信誉功能，可以阻止用户访问恶意Web站点；支持日志审查，捕获和分析系统日志，为组织提供审计证据。（须提供系统功能截图证明）  3、支持本地扫描和云安全扫描，具备本地病毒码和云端病毒码，支持实时扫描，预设扫描和、手动扫描和快速扫描。  4、对病毒的处理措施支持：清除、删除、拒绝访问、隔离、不予处理，系统针对不同的病毒类型提供默认配置，同时支持用户自定义。  5、★支持病毒检测，根据策略对病毒文件进行检测和告警，对病毒样本基本库至少能检测其中的95%，对病毒样本流行库至少能检测其中的98%；根据策略对病毒文件进行检测和告警，对误报样本库的误报率不能超过0.1%；支持对虚拟化环境中统一检测的策略管理,避免统一检测对虚拟化环境应用造成影响。支持即时保护、病毒阻断、病毒隔离；能根据安全策略对病毒文件进行清除，对病毒样本基本库至少能清除其中的90%，对病毒样本流行库至少能清除其中的95%。（上述功能提供具有CMA、CNAS标识的国家计算机病毒应急处理中心计算机病毒防治产品检验实验室出具的检验报告证明）  6、支持推荐扫描，根据不同计算机的扫描结果自动下发对应的入侵防御规则；支持快速定制入侵防御规则。（须提供系统功能截图证明）  7、支持扫描资源优化，手动扫描支持CPU资源使用率调整，当CPU超过阈值时暂停或者减少CPU使用率。可以设置CPU占用不高于50%或者20%；防病毒扫描支持VM扫描缓存和多线程处理。  8、★防火墙功能支持无代理方式部署，实现与NSX集成下发防火墙策略。（须提供系统功能截图证明）  9、具有应用程序控制功能，应用程序控制模块监控变化，一旦启用应用程序控制，将会记录所有软件更改，并创建事件。  10、支持完整性监控，能够监控操作系统和关键应用包括注册表项、关键目录、特定目录变更，以防范恶意修改。  11、支持对主机的日志审计，包括收集和分析操作系统和应用程序日志中的安全事件；支持多种系统事件记录，记录包括管理员、审计员、系统等所有审计日志。  12、★资质要求：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》虚拟化安全防护产品（增强级）；生产厂商具备CMMI 5级认证证书；生产厂商具备中国电子工业标准化技术协会颁发的ITSS《信息技术服务标准符合性证书》（业务领域：运行维护服务，评估等级：三级）； |  |  |
| **7** | Web  VPN设备 | 基本参数：提供并发用户数≥1000（永久授权）。 硬件部署，硬件需满足：至少3.4GHz四核8线程/16G/500G SSD/6个千兆电口,2U/冗余电源。  产品指标要求：  1、产品支持WEB VPN模块。产品应在无需安装客户端或控件情况下，在后端进行业务发布方式即可访问学校电子图书资源、OA、科研、财务、教务系统等各类B/S业务系统。产品支持客户登录成功，可以通过点击对应访问图标的方式进行一键式访问。  2、产品提供支持WEB终端。在不安装任何控件下，支持通过系统访问RDP、VNC、Telnet、SSH等协议资源；  针对RDP、VNC、Telnet、SSH等协议资源，支持管理员在系统中配置资源账号密码及授权用户，且该账密对用户透明；  ★4、针对RDP、VNC、Telnet、SSH等协议资源访问，支持其操作等记录与审计，包括用户账号、用户IP、操作资源、操作时间；且针对SSH、Telnet协议的资源访问，记录其全量操作指令，针对RDP、VNC协议的资源访问记录所有操作过程，且支持通过Web在线视频回放或下载至本地。（提供系统截图加盖公章）  ★5、产品需提供OAuth、CAS、短信认证、LDAP、RADIUS等认证方式。可针对用户支持密码、短信、邮件、等多因素认证，支持多种社交化认证方式，如企业微信、钉钉等。（需提供验证截图）  6、产品需提供学校统一认证平台的对接，实现校内校外统一认证平台的无感单点登录，用户登录统一认证门户之后，无需二次登陆访问业务。  7、针对HTTP、HTTPS协议的资源，支持单点登录功能，用户登录门户后再访问目标资源时，无须重复认证；无需针对基于HTTP/HTTPS的应用进行适配，包括绝对路径/特殊代码的适配、子域名/外链的适配、网站改版的更新适配。  8、产品需支持IPV4 /IPV6双栈接入访问，IPV4和IPV6互访。  9、产品需与门户系统、网上办事大厅等系统做深度融合，保证用户不受时间地点限制，内外网使用体验感完全一致。  （1）支持个性化门户（包括门户登录页、导航页内容、导航分组及分组内资源链接），可基于用户的访问权限展示其可访问资源导航，并支持用户自定义收藏夹内容；  （2）支持HTTPS类型Web资源的证书管理，且系统提供受浏览器信任的证书，对集成的门户及系统应用该SSL证书；  （3）支持根据用户角色、源地址、资源类型、待访问的资源地址四个方面对资源访问进行控制；支持校内资源外网访问（校内已购图书电子资源等）无需进行适配；  ★（4）支持判断用户的内外网环境，当用户在校内时，无需通过VPN直接访问网上办事大厅，当用户在校外时，自动加载VPN进行访问，并且直接跳转到办事大厅内，无需点任何图标或者链接，提供该功能的说明承诺函并加盖公章。  ★10、支持设置账号有效期，到期后禁止登录，支持管理员手动延长使用期限。（提供系统截图加盖公章）  产品提供不少于4路ISP网络接入到用户网络，实现不同ISP线路快速接入，并保障访问的源进源出能力  图书下载要求：  1、支持已购买的所有图书电子资源外网访问，无需进行适配；  ★2、支持对图书电子资源下载进行限速控制，当用户下载数量超过设定的阈值，给用户自动进行封禁，提供系统截图加盖公章；  ★3、为了方便图书馆进行电子资源访问统计，需要提供针对图书馆资源的报表功能，包括：电子资源访问统计报表、资源下载统计报表、关键字搜索统计报表、用户下载统计报表等，提供系统截图加盖公章。  信息安全要求：  ★4、产品能够有效阻止外部工具对内部业务系统的扫描探测，并针对所发布的浏览器应用进行URL地址伪装，防止服务器真实IP地址泄露，免遭恶意攻击，保障内部系统安全。且所有访问URL加密为不可逆方式连接，跨浏览器无法通过复制粘贴方式进行进一步访问。  5、产品支持DES、3DES、SHA、RSA等商用密码以及SM2、SM3、SM4国密算法保障传输安全。  6、产品客户端支持不依赖虚拟网卡方式建立隧道，从而减少系统的兼容性问题。  ★7、支持访问白名单机制，把不在访问策略范围内的资源直接通过原有路径进行访问。  ★8、支持地址轮询，通过多个IP轮询访问电子资源，且支持对特定资源进行流控,有效规避电子资源方将系统IP地址识别为恶意地址，提供系统截图加盖公章。  ★9、支持动态禁止频繁登录失败用户再次尝试，并支持自定义其失败频率阈值及禁止再次登录时间，提供系统截图加盖公章。  ★10、系统具备暴力防破解功能，支持自动异常登陆封禁IP、账号，支持管理员手动解封禁功能，提供系统截图加盖公章。  兼容性/用户端侧要求：  1、产品支持主流浏览器访问：chrome、firefox、360、qq、ie11+、edge等。  2、产品支持手机、笔记本电脑、台式电脑等终端使用，产品支持当前市面上主流的终端操作系统，如：Linux，Windows 7/8/10+，Mac，ios，Android。  系统要求：  1、支持在线升级系统且无需重启，保证业务的连续性；  2、配置数据、日志数据、性能数据分别采用专用数据库存储，优化数据存储结构，提升数据存取效率；  3、支持监控系统自身运行状态，包括CPU、内存、负载状态、网卡流量以及磁盘使用情况；  4、提供与操作系统、数据库以及其他平台软件深度整合的统一介质，能够实现操作系统、数据库、其他平台软件和系统的统一安装；  ★5、支持详细的账户控制策略，包括但不限于：登录时间策略、登录密码复杂度、多因子配置（提供产品截图）。  日志与报表：  ★6、支持记录与查询全量访问日志，包括用户账号、用户IP、终端、请求时间、访问URL、请求结果等，提供系统截图加盖公章；产品日志支持独立审计功能，产品日志需至少保留180天。  7、支持记录与查询全量登录日志，包括用户账号、用户IP、登录时间及登录结果；  ★8、支持多种日志分析维度（访问量、浏览器、操作系统、设备类型、请求来源地理位置等，并可根据时间段及不同时间维度（日、周、月、年）进行统计，通过可视化图表展示变化趋势）。（提供产品截图）  9、支持与专业的日志分析平台及态势感知等安全平台对接，可实现将以IP标识的日志转化为以终端+账号为标识。  服务要求：  提供三年原厂质保服务和免费升级服务； |  |  |
| **注：如以上招标参数中有明显偏向性和专有性参数，请投标单位在参数响应表中备注说明，评标过程中区别对待。** | | | | |

**附件二**

**投标主要标准文件格式**

**（一）投标封面格式**

**项目招标**

**投**

**标**

**文**

**件**

**招标编号：**

**项目名称：**

**投标文件内容： 商务标/技术标**

**投 标 人（联系方式）： （盖公章）**

**法定代表人或其委托代理人： （签字、盖章）**

**日 期： 年 月 日**

**（二）法定代表人身份证明书**

单位名称：

单位性质：

地 址：

成立时间： 年 月 日

经营期限：

姓 名： 性别： 年龄： 职务：

系 的法定代表人。

特此证明。

投标人：

日 期： 年 月 日

**（三）投标授权委托书**

本授权委托书声明：我（姓名） 系 （投标单位名称）的法定代表人，身份证号： ，现授权委托本单位： 的同志为我公司的合法代理人，就（项目名称） 的投标，以本公司的名义签署投标书，解释投标文件，进行合同谈判、签署合同及处理与之有关的一切事宜。

代理人无转委托权，特此委托。

代理人： （签字）性别： 年龄：

身份证号码： 职务：

投标人： （盖章）

法定代表人： （签字或盖章）

授权委托日期： 年 月 日

**（四）投标函**

致： ：

1、根据贵方的 项目招标文件，遵照《中华人民共和国招标投标法》等相关规定，经踏勘项目现场和研究上述招标文件、招标答疑及其他有关文件后；我方愿以**投标函**的报价完成招标文件要求的全部内容，不再计取任何其他费用。

2、我方已详细审核并确认全部招标文件及有关附件，充分理解投标报价不得低于企业个别成本有关规定我方经成本核算，所填报的投标报价不低于企业个别成本。

3、一旦我方中标，我方保证按 日历天供货周期完成合同约定的全部产品的供应，并通过招标人的验收。

4、一旦我方中标，我方保证产品质量达到 国家及行业相关质量要求的 质量等级。

5、一旦我方中标，我方保证在规定时间内按照招标文件中的《合同条款》由我方法定代表人亲自签订合同，认真履行合同和其他各项承诺。

6、我方同意所提交的投标文件在招标文件的投标须知中规定的投标有效期内有效，在此期间内如果中标，我方将受此约束。

7、除非另外达成协议并生效，你方的中标通知书和并投标文件以及招标文件、招标答疑、补充文件将成为约束双方的合同文件的组成部分。

8、我方承认投标函附录是我方投标函的组成部分，投标函附录附后。

投标人：

单位地址：

法定代表人或其委托代理人：

邮政编码： 电话： 传真：

开户银行名称：

开户银行账号：

开户银行地址：

开户银行电话：

**投标人签字盖章：**

日期： 年 月

1. **投标报价**

投标单位:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ 项目名称：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **序号** | **名称** | **数量** | **报价（元）** | **备注** |
| 1 | 上网行为管理 | 1项 |  |  |
| 2 | 数据库审计 | 1项 |  |  |
| 3 | 防火墙 | 1项 |  |  |
| 4 | WEB应用防护墙设备 | 1项 |  |  |
| 5 | 日志审计 | 1项 |  |  |
| 6 | 防病毒软件系统 | 1项 |  |  |
| 7 | WEB VPN设备 | 1项 |  |  |
| 3 | 合计总价： | |  |  |

**（六）投标报价说明**

（1）本报价依据本项目投标须知和合同文件的有关条款进行编制。

（2）产品报价包含产品价格、运输、保险、税费、装卸、施工、相关部门的检测、验收费用、成品保护、管理费、售后服务等全部费用，除非另有约定，招标人为履行本项目产品采购无需支付其他任何款项、费用。

（3）本分项报价表中的每一包项均应填写报价，对没有填写单价的项目费用，视为已包括在其他单价或合价之中。

（4）本报价的币种为：人民币 。

（5）投标人应将投标报价需要说明的事项，用文字书写与投标报价表一并报送。

投标人（公章）：

法定代表人或授权人签字：

**（七）项目建设管理及技术人员配置一览表**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **序号** | **姓名** | **职务** | **岗位职责** | **联系方式** | **身份证** | **备注** |
| **1** |  | **项目经理** |  |  |  |  |
| **2** |  | **技术负责人** |  |  |  |  |
| **3** |  | **施工人员** |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

**（八）投标报价需要说明的其他资料**

投标单位认为需对其投标报价进行其他补充说明及证明材料。

**附件三**

**保证承诺书**

**致安徽医科大学临床医学院：**

保证人 ，身份证号码 ，系 公司法定代表人/项目负责人。现保证人针对 公司与安徽医科大学临床医学院就 项目合作并签订《 合同》（下称主合同）事宜，为确保 公司全面履行其在主合同中的各项责任与义务，保证人自愿为其向安徽医科大学临床医学院提供不可撤销的连带保证责任担保，并向安徽医科大学临床医学院郑重承诺：

一、保证范围。保证人的保证范围，为主合同项下 公司对安徽医科大学临床医学院应承担的全部责任、义务、债务等，以及安徽医科大学临床医学院为实现债权而支付的各项费用（包括但不限于诉讼费/仲裁费、财产保全费、财产保全服务费、律师费、差旅费、公证费、执行费、公告费等费用）。

**二、保证期间**。保证人的保证期间，为 公司在主合同项下债务履行期限届满后三年；若主合同项下的债务约定分期履行的，则保证期间至 公司在主合同项下最后一期债务履行期限届满后三年。

**三、保证方式**。保证人承担独立的、不可撤销的、连带责任保证担保。任何情况下，不因主合同无效、撤销等等而影响本承诺书的效力。

四、保证人承诺，无论安徽医科大学临床医学院是否对被担保债权享有其他担保（包括但不限于保证、抵押、质押等），保证人在本承诺书项下的保证责任均不因此减免。安徽医科大学临床医学院均可直接要求保证人依照本承诺书约定承担保证责任，保证人不提出任何异议。

五、保证人是具备完全民事行为能力的自然人，保证人为签订本承诺书提供的所有文件、信息及签字均真实、完整、有效 。

六、保证人已充分理解并全面认可主合同及本承诺书的所有条款内容，并承诺任何情况下不得对其提出任何异议。

保证人：

日期：

**附件四**

**廉 政 承 诺 书**

甲方：

乙方：

为加强甲乙双方合作及廉政建设，规范甲乙双方各项合作行为，预防发生各种谋取不正当利益的违法违纪行为，保护双方合法权益，根据国家有关法律法规和新华集团相关文件规定，特订立本廉政承诺书。

第一条 甲乙双方共同承诺

（一）严格遵守国家关于市场准入、项目招标投标、工程建设、施工安装、物资采购和市场活动等有关法律、法规和相关政策，以及廉政建设的各项规定。

（二）严格执行合同文件，自觉按合同办事。

（三）坚持公开、公平、公正的原则，不为获取不正当利益而损害对方利益。

（四）保守对方的商业秘密，不将其用于交易以外的目的。

第二条 甲方承诺

在交易的事前、事中、事后遵守以下（包括但不限于）事项：

（一）不参加乙方或相关单位的宴请。

（二）不私自收受乙方或相关单位的礼品、礼券或以“低价付款”的物品。

（三）不接受乙方或相关单位的礼金、贿赂、帐外回扣等任何形式的私下经济利益。

（四）不私自接受乙方或相关单位提供的娱乐、游玩或任何考察形式的变相旅游等活动。

（五）不利用职务之便谋取非法利益；不向乙方或相关单位介绍配偶、子女及其他亲属参与同交易有关的经济活动；不以任何理由向乙方或相关单位推荐分包单位、供货商，或要求乙方购买交易合同规定以外的材料、设备等。

（六）不得有其他任何在乙方等相关单位获取不当利益的行为。

第三条 乙方承诺

在交易的事前、事中、事后遵守以下（包括但不限于）事项：

（一）与甲方保持正常的业务交往，严格执行合同约定。

（二）不向甲方工作人员及任何与甲方相关联的单位或个人提供宴请、旅游、健身、娱乐、变相考察等活动。

（三）不私自向甲方、相关单位及其工作人员赠送礼品、现金、有价卡券等。

（四）不在帐外给予甲方、相关单位及其工作人员回扣；不假借促销费、宣传费、赞助费、科研费、劳务费、咨询费、好处费、感谢费、佣金等名义，或者以报销各种费用等方式，给付甲方、相关单位及其工作人员财物（利益）。

（五）及时向甲方通报甲方人员违反本承诺书规定的行为。

第四条 违约责任

（一）甲方工作人员违反本承诺书第一条、第二条的，严格按甲方相关公司制度处理和有关法律法规处理;涉嫌犯罪的，移交司法机关处理；给乙方造成经济损失的，责任人应予以赔偿。

（二）乙方工作人员违反本承诺书第一条、第三条的，按乙方相关制度和有关法律法规处理，甲方有权终止合同;涉嫌犯罪的，移交司法机关处理；给甲方造成经济损失的，乙方承担赔偿责任。

第五条 本承诺书作为交易合同或协议的附件，与交易合同或协议具有同等法律效力。经双方签署后立即生效。

第六条 乙方在履行合同或协议过程中，若发现甲方的相关人员有违反《廉政承诺书》所规定的行为，可以直接向甲方审计督查部投诉（电话：15005518562）。

第七条 本承诺书一式五份，甲方持四份，乙方持一份。

甲方单位：（盖章） 乙方单位：（盖章）

法定代表人： 法定代表人：

法定代表人联系电话： 法定代表人联系电话：

委托代理人： 委托代理人：

项目负责人： 项目负责人：

监督电话：15005518562 监督电话：

监督邮箱：xhjtdc@xinhuaedu.com 监督邮箱：

jtdsz@xinhuaedu.com