招　标　文　件

项目名称：	桂林医学院附属医院一院两区网络安全建设项目
项目编号：	**GXZC2023-G3-003411-JDZB**
联系电话：	**0773-3696789 转 2**

采购人：　桂林医学院附属医院

采购代理机构：　广西机电设备招标有限公司

2023 年　月

目　　录

第一章　招标公告

广西机电设备招标有限公司关于桂林医学院附属医院一院两区网络安全建设项目(GXZC2023-G3-003411-JDZB)公开招标公告

项目概况

桂林医学院附属医院一院两区网络安全建设项目招标项目的潜在供应商应登录政采云平台 （http：//www.zcygov.cn）在线申请获取招标文件，并于 2023 年　月　日 9 点 30 分（北京时间）前递交投标文件。

一、项目基本情况

项目编号：GXZC2023-G3-003411-JDZB

项目名称：桂林医学院附属医院一院两区网络安全建设项目

预算总金额（元）：7000000

采购需求：

标项名称：桂林医学院附属医院一院两区网络安全建设项目

数量：1

预算金额（元）：7000000

简要规格描述或项目基本概况介绍、用途：桂林医学院附属医院一院两区网络安全建设项目 1 项。如需进一步了解详细内容，详见招标文件。

最高限价（元）：7000000

合同履行期限：自签订合同之日起 180 个日历日内完成网络安全建设。

本标项（否）接受联合体投标

备注：

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；

2.落实政府采购政策需满足的资格要求：本项目非专门面向中小微企业采购。

3.本项目的特定资格要求：

（1）资质要求：无。

（2）业绩要求：无。

（3）其他要求：无。

（4）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，不得参加本项目同一合同项下的政府采购活动。为本项目提供整体设计、规范编制或者项目管理、监理、检测等服务的供应商，不得再参加本项目的采购活动。

（5）未被列入失信被执行人、重大税收违法失信主体、政府采购严重违法失信行为记录名单。

（6）本项目不允许分包。

（7）本项目不接受联合体投标。

（8）按照招标公告规定获得招标文件。

三、获取招标文件

时间：2023 年　月　日至 2023 年　月　日 ，每天上午 00:00 至 12:00，下午 12:00 至 23:59（北京时间，法定节假日除外）

地点（网址）：政采云平台 （http：//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：2023 年　月　日 09:30（北京时间）

地点（网址）：通过政采云平台实行在线投标。

开标时间：2023 年　月　日 09:30

开标地点：通过政采云平台实行在线解密开启。

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.公告发布媒体：广西政府采购网、中国政府采购网

2.需落实的政府采购政策：本项目适用政府采购促进中小企业、监狱企业发展、促进残疾人就业、信息安全产品等有关政策，具体详见招标文件。

3.投标文件解密时间：截标时间后 30 分钟内（2023 年　月　日上午 9 时 30 分至 10 时 00 分）供应商可以登录政采云平台，用“项目采购-开标评标”功能进行解密投标文件。若供应商在规定时间内无法解密或解密失败，可以以电子备份投标文件作为依据【在接到无法解密或解密失败的通知后，供应商可根据自身实际情况按通知时要求的时间到桂林市公共资源交易中心　号开标室现场提交或以电子邮件的形式（以通知时所告知的电子邮箱地址为准）提交电子备份投标文件】，若供应商在规定时间内无法解密或解密失败且未提供电子备份投标文件的（包含提供的电子备份文件无效或无法解密的情况），视为投标无效。

4.“政采云”平台电子投标相关事宜：

（1）未进行网上注册并办理数字证书（CA 认证）的供应商将无法参与本项目政府采购活动，潜在供应商应当在响应截止时间前，完成政采云平台上的 CA 数字证书办理及投标文件的提交。完成 CA 数字证书办理预计 7 日左右，建议各供应商抓紧时间办理。

（2）为确保网上操作合法、有效和安全，请供应商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章，妥善保管 CA 数字证书并使用有效的 CA 数字证书参与整个招标活动。

（3）若对项目采购电子交易系统操作有疑问，可登录“政采云”平台（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点击右侧帮助文档查看供应商指南或拨打政采云服务热线 95763 获取热线服务帮助。

七、对本次招标提出询问，请按以下方式联系

1、采购人信息

名称：桂林医学院附属医院

地址：桂林市秀峰区乐群路 15 号

项目联系人：蒋老师

项目联系方式：0773-2802050

邮箱：gyzbcg@163.com

2、采购代理机构信息

名称：广西机电设备招标有限公司

地址：桂林市骖鸾路 31 号湘商大厦 6 楼 603（桂林分公司）

项目联系人：曾昭卉

联系方式：0773-3696789 转 2

广西机电设备招标有限公司

2023 年　月　日

第二章　采购需求

一、总体要求

1.需实现的功能、目标及应用场景

满足采购文件要求，验收达到合格标准。

2.政府采购政策的应用

详见采购文件“评标方法及评标标准/政府采购政策应用说明”。

3.是否接受进口产品：

本项目采购货物均不接受进口产品。

4.需执行的国家相关标准、行业标准、地方标准或者其他标准、规范

（1）本项目应执行的国家相关标准、行业标准、地方标准或者其他标准、规范为：____/____

（2）如技术要求/服务要求与上述标准、规范不一致的，高于标准、规范的按技术要求执行，低于标准、规范的按标准、规范执行。

5 标注“▲”的条款或要求系指实质性条款或实质性要求，必须满足，如存在负偏离将导致投标被否决。

6.标注“★”项的技术参数为本次采购重要参数条款，非实质性要求，负偏离作为扣分项。

7.采购需求要求未尽事宜由采购人与中标供应商在采购合同中约定。

8.标的所属行业：软件和信息技术服务业。

二、技术要求

1.一般说明

（1）本表中如提及品牌型号，仅起参考作用。供应商可选用其他品牌型号替代，但这些替代的品牌型号要实质上参照或相当于或优于参考品牌型号及其技术参数性能（配置）要求。

（2）如要求提供检测报告的，检测报告或认证报告内容中若涉及外文说明，必须同时提供对应中文翻译说明，评标依据以中文翻译内容为准，外文说明仅供参考；产品检测报告应为报告正面、背面和附件标注的全部具体内容；产品检验报告的尺寸和清晰度应该能够在电脑上被阅读、识别和判断。

2.本项目核心产品：第 1 项 出口防火墙。

3.标的名称、数量、需满足的质量、技术规格、物理特性、性能、材料、结构、外观、安全，或者服务内容和标准

项号	货物名称	单位	数量	技术参数
1	出口防火墙	台	4	1.标准 2U 设备，冗余电源；配置不少于 8 个 10/100/1000M 自适应电口，不少于 8 个千兆光口（配置 8 个千兆多模光模块），另有≥1 个接口板卡扩展插槽，≥256GB SSD 硬盘。含≥3 年硬件质保。

				2.防火墙吞吐≥10Gbps，并发连接数 250 万，每秒新建连接数 15 万/秒，支持应用控制、URL 过滤、病毒防护、入侵防御、威胁情报检测等功能模块。配置≥3 年防病毒、入侵防御特征库升级服务。 3.所投产品支持 MPLS 流量透传；支持针对 MPLS 流量的安全审查，包括漏洞防护、反病毒、间谍软件防护、内容过滤、URL 过滤、基于终端状态访问控制等安全防护功能。 4.投产品支持基于策略的路由负载，支持根据应用和服务进行智能选路，支持源地址目的地址哈希、源地址哈希、轮询、时延负载、备份、随机、流量均衡、源地址轮询等路由负载均衡方式。 5.所投产品支持 DDNS 功能，支持 Oray 向日葵、Pubyun 公云、Noip、Changeip 提供的 DDNS 服务，将动态获取的 IP 地址映射为固定的域名。 6.所投产品支持在虚拟系统内独立配置病毒防护、漏洞利用防护、间谍软件防护、URL 过滤、文件过滤、内容过滤、邮件过滤、行为管控等安全功能。并可支持对本虚系统内产生的日志进行独立审计。 7.所投产品支持基于源安全域、目的安全域、源用户、源地址、源地区、目的地址、目的地区、服务、应用、隧道、时间、VLAN 等多种方式进行访问控制，并支持地理区域对象的导入以及重复策略的检查。 8.所投产品支持灵活的服务链编排功能，支持串接链和旁路链，支持网元组的方向和位置设置。 9.所投产品支持灵活的细粒度引流策略，可基于源安全域、目的安全域、源用户、源地址、目的地址、服务、VLAN、服务链、流量方向（内网到外网/外网到内网）的引流策略，并详细记录日志。
2	管理区防火墙	台	3	1.标准 1U 设备，冗余电源；配置不少于 8 个 10/100/1000M 自适应电口，不少于 2 个千兆光口（配置 4 个千兆多模光模块），不少于 4 个万兆光口接口，另有≥1 个接口板卡扩展插槽，1 个 Console 口，≥256GB SSD 硬盘。含≥3 年硬件质保。 2.防火墙吞吐≥6Gbps，并发连接数≥200 万，每秒新建连接数≥8 万/秒，包含应用控制、URL 过滤、病毒防护、入侵防御、威胁情报检测等功能模块。配置≥3 年防病毒、入侵防御特征库

				升级服务； 3.具备端口映射功能。 4.所投产品支持 MPLS 流量透传；支持针对 MPLS 流量的安全审查，包括漏洞防护、反病毒、间谍软件防护、内容过滤、URL 过滤、基于终端状态访问控制等安全防护功能。 5.所投产品支持基于策略的路由负载，支持根据应用和服务进行智能选路，支持源地址目的地址哈希、源地址哈希、轮询、时延负载、备份、随机、流量均衡、源地址轮询等路由负载均衡方式 6.★所投产品支持在源地址转换过程中，对 NAT（源地址转换）使用的地址池利用率进行监控，并在地址池利用率超过阈值时，通过 SNMP Trap、邮件等方式告警**（投标文件需提供能够体现上述功能配置选项截图复印件）**。 7.所投产品支持 DDNS 功能，支持 Oray 向日葵、Pubyun 公云、Noip、Changeip 提供的 DDNS 服务，将动态获取的 IP 地址映射为固定的域名。 8.所投产品支持 DS-Lite CPE B4 功能，支持成为 b4 或 aftr 角色，支持从 DHCPv6 服务器或手动方式获取 AFTR 参数。 9.所投产品支持在虚拟系统内独立配置病毒防护、漏洞利用防护、间谍软件防护、URL 过滤、文件过滤、内容过滤、邮件过滤、行为管控等安全功能。并可支持对本虚系统内产生的日志进行独立审计。 10.所投产品支持基于源安全域、目的安全域、源用户、源地址、源地区、目的地址、目的地区、服务、应用、隧道、时间、VLAN 等多种方式进行访问控制，并支持地理区域对象的导入以及重复策略的检查。 11.★所投产品支持共享上网检测功能，可以通过设置管控地址和例外地址优化管控功能，同时支持阻断或告警动作**（投标文件需提供能够体现上述功能配置选项截图）**。 12.所投产品支持将其他硬件安全设备（包括但不限于防火墙、IPS、IDS、WAF、行为管理、流量探针等）加入网元组，并接受流量编排；支持将同类型安全设备划归同一网元组，组成硬件安全资源池（如 WAF 安全资源池），并将流量通过负载均衡（“源地址哈希”、“源目的地址哈希”，“加权源地址哈希”、“加权源目的地址哈希”、“加权地址端口哈希”、“轮询”和“权重轮询”）

				的方法编排给组内所有网元。 13.所投产品支持灵活的服务链编排功能，支持串接链和旁路链，支持网元组的方向和位置设置。 14.所投产品支持灵活的细粒度引流策略，可基于源安全域、目的安全域、源用户、源地址、目的地址、服务、VLAN、服务链、流量方向（内网到外网/外网到内网）的引流策略，并详细记录日志。 15.★所投产品支持对编排的流量进行监控，至少能从网元组、引流策略两个维度对编排流量监控统计。**（投标文件需提供能够体现上述功能配置选项截图）** 16.所投产品支持基于不同安全区域防御 SYN Flood、UDP Flood、ICMP Flood、IP Flood、DNS Flood、HTTP Flood、NTP Query Flood 、NTP Reply Flood 和 SIP Flood 攻击，并支持警告、丢弃、普通防护（首包丢弃）、增强防护（TC 反弹技术）、授权服务器防护（NS 重定向）、普通防护（自动重定向）、增强防护（手工确认）等多种防护措施。 17.所投产品支持 DHCP 协议防护；支持手动定义可信 DHCP 服务器 IPv4 和基于阈值限制 DHCP 请求传输速率。 18.所投产品支持 IPv4 和 IPv6 流量的 HTTPS、POP3S、SMTPS、IMAPS 协议进行解密，支持配置基于源安全域、目的安全域、源地址、目的地址、SSL 协议服务的解密策略，动作可以设置解密或不解密。 19.所投产品支持 IPv4 和 IPv6 流量的蜜罐引流策略，支持配置基于源安全域、目的安全域、源地址、目的地址、服务、VLAN 的引流策略，并支持强制导流，能够通过设置服务器和端口进行引流。 20.★产品支持与杀毒软件或终端管理软件联动，实现基于终端健康状态的访问控制**（投标文件需提供能够体现上述功能配置选项截图复印件）；**
3	数据中心防火墙	台	4	1.★标准 2U 设备，冗余电源；配置≥8 个千兆电口，≥8 个千兆光口，≥8 个万兆光口（含 8 个万兆多模光模块）；标准配置 1 个 Console 口、1 个 HA 接口、1 个 MGT 接口，具备液晶屏，≥256GB SSD 硬盘。含≥3 年硬件质保。 **2.▲防火墙吞吐≥42Gbps，并发连接≥580 万，每秒新建连接数≥50 万，支持应用控制、URL 过滤、病毒防护、入侵防御、**

				威胁情报检测等功能模块。配置≥3 年防病毒、入侵防御特征库升级服务； 3.所投产品支持 MPLS 流量透传；支持针对 MPLS 流量的安全审查，包括漏洞防护、反病毒、间谍软件防护、内容过滤、URL 过滤、基于终端状态访问控制等安全防护功能。 4.所投产品支持基于策略的路由负载，支持根据应用和服务进行智能选路，支持源地址目的地址哈希、源地址哈希、轮询、时延负载、备份、随机、流量均衡、源地址轮询等路由负载均衡方式。 5.所投产品支持在源地址转换过程中，对 NAT（源地址转换）使用的地址池利用率进行监控，并在地址池利用率超过阈值时，通过 SNMP Trap、邮件等方式告警。（投标文件需提供能够体现上述功能配置选项截图复印件） 6.所投产品支持 DDNS 功能，支持 Oray 向日葵、Pubyun 公云、Noip、Changeip 提供的 DDNS 服务，将动态获取的 IP 地址映射为固定的域名。 7.所投产品支持 DS-Lite CPE B4 功能，支持成为 b4 或 aftr 角色，支持从 DHCPv6 服务器或手动方式获取 AFTR 参数。 8.所投产品支持在虚拟系统内独立配置病毒防护、漏洞利用防护、间谍软件防护、URL 过滤、文件过滤、内容过滤、邮件过滤、行为管控等安全功能。并可支持对本虚系统内产生的日志进行独立审计。 9.所投产品支持基于源安全域、目的安全域、源用户、源地址、源地区、目的地址、目的地区、服务、应用、隧道、时间、VLAN 等多种方式进行访问控制，并支持地理区域对象的导入以及重复策略的检查。 10.所投产品支持共享上网检测功能，可以通过设置管控地址和例外地址优化管控功能，同时支持阻断或告警动作。（投标文件需提供能够体现上述功能配置选项截图复印件） 11.所投产品支持将其他硬件安全设备（包括但不限于防火墙、IPS、IDS、WAF、行为管理、流量探针等）加入网元组，并接受流量编排；支持将同类型安全设备划归同一网元组，组成硬件安全资源池（如 WAF 安全资源池），并将流量通过负载均衡（“源地址哈希”、“源目的地址哈希”，“加权源地址哈希”、“加权源目的地址哈希”、“加权地址端口哈希”、“轮询”和“权重轮询”）

				的方法编排给组内所有网元。 12.所投产品支持灵活的服务链编排功能，支持串接链和旁路链，支持网元组的方向和位置设置。 13.所投产品支持灵活的细粒度引流策略，可基于源安全域、目的安全域、源用户、源地址、目的地址、服务、VLAN、服务链、流量方向（内网到外网/外网到内网）的引流策略，并详细记录日志。 14.★所投产品支持对编排的流量进行监控，至少能从网元组、引流策略两个维度对编排流量监控统计。**（投标文件需提供能够体现上述功能配置选项截图复印件）** 15.所投产品支持基于不同安全区域防御 SYN Flood、UDP Flood、ICMP Flood、IP Flood、DNS Flood、HTTP Flood、NTP Query Flood 、NTP Reply Flood 和 SIP Flood 攻击，并支持警告、丢弃、普通防护（首包丢弃）、增强防护（TC 反弹技术）、授权服务器防护（NS 重定向）、普通防护（自动重定向）、增强防护（手工确认）等多种防护措施。 16.所投产品支持 DHCP 协议防护；支持手动定义可信 DHCP 服务器 IPv4 和基于阈值限制 DHCP 请求传输速率。 17.所投产品支持 IPv4 和 IPv6 流量的 HTTPS、POP3S、SMTPS、IMAPS 协议进行解密，支持配置基于源安全域、目的安全域、源地址、目的地址、SSL 协议服务的解密策略，动作可以设置解密或不解密。 18.★所投产品支持 IPv4 和 IPv6 流量的蜜罐引流策略，支持配置基于源安全域、目的安全域、源地址、目的地址、服务、VLAN 的引流策略，并支持强制导流，能够通过设置服务器和端口进行引流**（投标文件需提供能够体现上述功能配置选项截图）**。 19.所投产品支持将告警信息以 SNMP Trap、邮件、声音、短信等形式通知管理员，告警信息的范围至少包括配置变更、病毒事件、攻击事件、异常事件、失陷主机告警、并发数告警、CPU 利用率、内存利用率、硬盘利用率、接口带宽利用率、NAT 端口池利用率等； 20.支持作为轻量级“探针”与本项目中配置的威胁感知系统联动，上报网络活动产生的数据至网络威胁感知系统；并支持接收来自网络威胁感知系统推送的处置策略，及时拦截绕过防御措施产生的高级威胁。

4	终端安全管理系统	套	1	1.软件形式交付，包含控制中心和客户端软件。控制中心能够实现对客户端的集中管理，包括终端统一部署、策略配置、任务分发、集中监控、日志报表等功能；支持根据客户端点数的增加进行横向扩展；具备防病毒、补丁管理、主机防火墙、终端管控等功能，含≥3000 个 windows 客户端授权；提供≥3 年的特征库升级及维保服务。 2. 操作系统： Windows XP_SP3 及以上 /Windows Vista/Windows 7/Windows 8/Windows 10/windows 11。 3.支持终端用户和管理员是一套账号管理系统，简化账号管理复杂度，一个账号解决所有身份认证，既可以用于终端登录，也可以用于管理管理中心。 4.★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**（投标文件需提供能够体现上述功能配置选项截图复印件）**。 5.客户端主程序、病毒库版本支持按分组和多批次进行灰度更新，保持在低风险中完成终端能力更新。支持设置不同终端类型设置和每批次观察时长。当检测到新版本将从第一批次重新观察。 6.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。 7.★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**（投标文件需提供能够体现上述功能配置选项截图复印件）。** 8.支持自动阻止远程登录行为，防护黑客远程爆破和拦截恶意的远程登录。 9.支持无文件攻击防护、文档攻击防护、横移渗透攻击防护、内存攻击防护。 10.支持不少于三个杀毒引擎混合使用，提高病毒检出率。 11.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。 12.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。 13.支持开启自动修复漏洞，包括开机时修复，并支持随机延迟执行、间隔修复和按时间段修复，可设置延迟时间、间隔修复时间和修复时间段。 14.支持按照补丁的维度统计补丁安装情况，包括补丁号、系统类型、补丁类型、补丁级别、补丁名称、补丁描述、发布日期、发布状态、文件数量、发现补丁次数、已安装补丁次数、忽略补丁次数、卸载补丁次数、未更新补丁库。并支持导出统计报表。 15.★支持预先设置好补丁灰度发布批次漏洞修复策略，每当控制台更新补丁库，根据企业环境自动先推送给第一个小批次分组，如无问题自动推送给下一个批次，直到推送给全网（**投标文件需提供能够体现上述功能配置选项截图复印件）。** 16.支持主机防火墙功能，通过添加 IP、域名规则、支持允许/拒绝规则、支持任意流向拦截和允许，支持 TCP、UDP、TCP+UDP、ICMP、多播和组播，支持自定义端口范围、支持自定义目标 IP，支持输入 IP 范围。 17.支持展示防火墙上报日志，展示终端基础信息、拦截规则名称、拦截时间、操作、协议、源地址，目的 IP/域名、源端口、目的端口。 18.★支持对外设进行多维度的放行，包括设备名称、PID/VID、实例路径，通过添加实现例外或加黑（**投标文件需提供能够体现上述功能配置选项截图复印件）。** 19.支持对终端节能管理，支持对长时间运行、定时关机、空闲节能、工作时间外开机等节能类型设定策略，支持仅提示、关机、注销、锁定、关闭显示器、锁定+关闭显示器、休眠和睡眠处理。并支持提示倒计时弹窗，可设置在终端取消后下一次提醒时间。 20.支持对网卡进行防护，支持阻止终端修改 IP 地址、使用动态 IP 地址、热点创建和 IPV6 地址使用等，可自定义提示内容和生效时间。 21.为了简便运维，要求终端安全管理系统支持与本项目网络准入认证系统在同一管理后台进行维护配置管理。 22.终端安全管理系统支持联动安装零信任客户端、可以自定义零信任客户端菜单名称，终端安全管理系统支持使用零信任

				认证信息自动登陆。
5	网络准入认证系统	套	1	1.标准 2U 设备,交流冗余电源，配置不少于 6 个千兆以太网电口，不少于 2 个万兆光口，≥2 个扩展槽；吞吐量≥8Gbps，硬盘≥2TB，配置≥2500 个准入终端用户许可授权；含≥3 年硬件质保及网络准入功能升级服务。 2.设备类型识别：通过快速扫描方法，实现对网络中视频设备及其他设备数量和类型的分类统计，能够识别包括摄像头、NVR、DVR、存储服务器及其他计算机、交换机、服务器、移动终端等设备类型。 3.视频设备信息采集：能够准确获取各类网络视频摄像机厂商及型号，覆盖海康威视、大华、宇视、科达、天地伟业、华为、安巡视、罗普特、索尼、菲力尔、英飞拓、云天励飞、英迪高、汉邦高科、乔安科技、易视云、华迈等市场主流视频设备厂商。 4.通讯关系展示：以图形化形式展示网络内设备与设备之间的网络通讯关系，基于图形化数据可直观定位关键应用设备。 5.识别库管理：支持指纹库管理，对于未识别成功的终端，可通过人工录入指纹的方式修正终端信息扫描结果，支持指纹库的外部导入及备份。能够同时根据 MAC 规则、操作系统、厂商、开放端口、运行服务、主机名、型号来自定义识别规则。 6.终端位置：终端位置支持网络内终端位置信息的展现，可准确展示终端所处交换机的 ip 及交换机具体端口数。当终端位置发生变更时，支持以邮件或短信方式通知管理员。 7.网络拓扑管理：图形化展示网络拓扑，直观地展示网络设备之间的连接关系。 8.★地址冲突发现：支持发现网络内的地址冲突事件，支持发现冲突设备的 MAC 和接入位置。**（投标文件需提供能够体现上述功能配置选项截图复印件）** 9.网中网发现：支持发现网络内的 NAT 设备，支持发现 NAT 网络内部设备信息。 10.准入技术：产品支持多种认证控制方式，支持 802.1x、portal、DHCP、MAB MAC、旁路镜像、WebAuth 等方式，支持无线和有线环境下的接入控制，适应复杂网络环境下的接入控制。 11.引导部署：支持检测是否安装客户端，达到入网遵从条件，保障入网终端是安全可信的，未安装客户端的终端禁止访问，

				将被重定向到客户端安装页面快速引导部署。针对未认证或不合规的设备，当终端访问 http、https 网站时，支持对其网站访问重定向至引导页面进行身份认证或修复。 12.★第三方认证源：支持 LDAP、Email、Http 认证源三种认证源配置。**（投标文件需提供能够体现上述功能配置选项截图复印件）** 13.支持员工扫描访客二维码和短信方式快速审批访客入网的访客认证方式。 14.设备身份认证：支持与同品牌终端安全管理系统联动，校验终端是否安装终端安全管理系统服务器下载的客户端，支持基于终端身份标识的设备身份验证方式，支持同时校验用户身份和设备身份的双重认证。**（投标文件需提供能够体现上述功能配置选项截图复印件）** 15.针对摄像头等低风险设备，允许未经审批的设备临时入网一段时间。方便设备抢修等应急事件。 16.NAT 精度控制入网：通过小路由、VPN 等场景接入的经过 NAT 转换后的终端必须安装客户端并经过身份认证后方可接入网络。 17.IP-MAC 绑定：支持手动或自动学习 IP/MAC 绑定关系，通过配置策略可对网络内设备随意变更 IP 地址的行为或随意使用其他设备 IP 地址的行为进行快速发现和有效阻断。 18.动态授权：可基于用户角色、设备标签、设备分组、终端安检结果等动态下发 VLAN、acl 或厂家属性。 19.动态 ACL：支持基于不同设备类型定义访问控制规则，特定类型的设备仅允许访问指定的关键服务器，并只允许合法的协议通过；支持基于终端使用用户的用户组、用户角色定义访问控制策略，无论用户使用什么设备还是 IP，均可执行对应的访问控制策略。 20.支持不安装客户端的合规检查功能，包括检查终端开放端口情况、检查终端外在静态指纹特征、检查设备协议、检查终端网络行为、异常流量检查、支持应用检查。 21.支持安装客户端的合规检查功能，包括认证方式、全静默认证、合规检查、隔离处置、引导修复、进程检查、域检查、共享文件检查、补丁检查、U 盘运行检查、注册表检查、软件检查、Guest 检查、操作系统检查、非法外联检查、IP 获取方式检

				查、防火墙检查、远程桌面检查、计算机名检查等 22.系统需具备多种逃生机制，一键认证放行、阈值检测逃生、第三方服务器异常自动放行，确保非正常情况下不影响用户网络的稳定运行。 23.便于运维人员管理，要求网络准入认证系统支持与本项目终端安全管理系统与在同一管理平台进行管理。**（投标文件需提供能够体现上述功能配置选项截图复印件）** 24.★支持与本项目威胁感知系统联动，对于第三方平台发现的风险终端，提供准入阻断的能力。**（投标文件需提供能够体现上述功能配置选项截图复印件）**
6	日志审计系统	台	1	1.标准 1U 机箱，配置不少于 6 个 10/100/1000M Base-T 自适应电口，≥2 个扩展槽，带 1 个 Console 口，4TB 磁盘存储硬盘；事件采集性能≥3000EPS，提供 100 个审计节点授权许可。提供≥3 年硬件质保和软件升级服务。 2.采用 B/S 模式，无需安装客户端，使用 WEB 浏览器访问管理中心，浏览器端无需安装 Java 运行环境。支持 chrome 浏览。 3.支持通过 Syslog、SNMP Trap、Netflow V5、ODBC/JDBC、Agent 代理(Windows/Linux)、WMI、(S)FTP、文件共享(SMB、NetBIOS)、文件\文件夹读取、Kafka 等多种方式完成各种日志的收集功能，支持多行日志采集合并为一行。 4.支持自定义资产类型及资产属性；支持对资产自定义标签，支持对标签内容进行查询和管理。 5.★支持对资产 IP 地址（含内网 IP）的地理信息进行管理，设置单 IP 及 IP 段行政区及经纬度**（投标文件需提供能够体现上述功能配置选项截图复印件）。** 6.系统提供页面可视化编辑归一化策略，对页面查看的日志编辑归一化策略，所见即所得，也支持通过归一化文件的导入来支持归一化，不需修改系统程序。 7.支持正则表达式、Key-Value、JSON 日志解析，支持日志自动化辅助范化。 8.★针对匹配的多条范化策略，系统支持用户手工设置策略匹配优先级**（投标文件需提供能够体现上述功能配置选项截图复印件）。** 9.日志解析字段内置≥130 个字段，属性字段可扩展，用户

				可根据审计需要自行创建字段，字段类型包括 IP、字符串、整型等 15 种，可选择映射函数等。内置及新增的所有字段均可参与查询、关联分析和报表统计。 10.★能够在世界地图上实时定位事件源/目的 IP 地址的地理位置（**投标文件需提供能够体现上述功能配置选项截图复印件**）。 11.支持对日志中的源和目的 IP 地址进行自动补全，补全 IP 地址的资产、国家、区域和城市等信息。 12.系统支持即席在线查询，支持嵌套查询，可针对查询结果任意回退，收敛事件范围；用户可根据需要配置事件显示的字段内容等。查询结果可支持加密导出。 13.可以以图形化的方式展示日志属性之间的聚合关系，并支持手动选择日志属性，显示多维事件分析图；属性可增加或减少，且支持图片大小调整。 14.支持将统计结果保存为仪表板、报表和策略，提供可编辑的灵活强大的自定义仪表板。 15.系统支持提供安全运维报告，帮助运维人员快速生成日常日志分析和运维报告。
7	堡垒机	台	1	1.标准 2U 机架式，标配不少于 4 个千兆电口、不少于 4 个千兆光口,支持≥1 个扩展插槽；采用多核硬件平台和国产服务器版操作系统，内置国密密码卡，支持 SM1、SM2、SM3、SM4、SM7、SM9 等密码算法，≥4TB 企业级硬盘，冗余电源。具备液晶屏，最大可选 500 授权许可，实配≥100 个授权，配置≥5 个智能密码钥匙（内置个人 CA）。含≥3 年维保服务。 2.设备采用旁路部署，不得影响业务环境，支持 HA 双机部署，支持集群部署，支持跨地域、跨数据中心分级部署，支持异地灾备部署。 3.★支持微信小程序动态口令认证方式登录堡垒机，且当用户需要使用手机令牌登录时，需要强制绑定手机令牌（**投标文件需提供能够体现上述功能配置选项截图复印件**）。 4.支持应用发布防跳转功能，进行 http/https 访问过程时运维人员仅允许访问授权地址。 5.支持云主机资源批量导入，包括阿里云、百度云、华为云、腾讯云、Ucloud、AWS、Azure 云平台的资源，支持设置优先导入公网和内网 IP 设置，支持导入同时批量新建标签。

				6.支持对数据库协议访问操作进行控制，可基于库、表、命令实现对数据库操作的细粒度访问控制，执行动作包括但不限于断开连接、拒绝执行、动态授权、允许执行。 7.★不限操作系统类型，无需安装任何客户端插件，使用浏览器通过 H5 方式即可直接运维 SSH、RDP、VNC、SFTP 资源**（投标文件需提供能够体现上述功能配置选项截图复印件）**。 8.支持 H5 运维过程中通过群发命令，实现同时运维多台资源设备。 9.支持运维过程中邀请其他用户参与、协助操作；会话协同过程中，协同者可以申请控制会话，创建者可以强制获取控制权。 10.★支持以云盘形式在堡垒机上存储常用文件，实现文件共享**（投标文件需提供能够体现上述功能配置选项截图复印件）**。 11.申请工单支持文件管理、RDP 剪切板、磁盘映射、键盘审计、剪切板审计（上行、下行）、显示水印、上传、下载权限、OCR 识别申请。 12.支持工单审批时，设置多级审批模式，需要逐级进行审批，最大支持 5 级。 13.支持水印功能，用户在运维或者是监控、查看会话时，H5 页面会将用户的登录名作为水印展示，避免数据泄露无法追责，支持在 H5 运维 SSH、RDP、TELNET、VNC、应用发布等资源时显示水印。 14.产品需支持专属手机 App 远程管理（非浏览器方式），可在 App 端实现用户管理、主机管理、工单审批、告警消息、会话管理等功能。 15.堡垒机内置文件病毒扫描能力，实现本地上传文件到堡垒机网盘、主机上传文件到堡垒机网盘的文件传输扫描，针对病毒文件，可以执行信任、删除等操作，并生成审计记录。
8	服务器安全管理系统	套	1	1.★管理控制中心软件，可实现对客户端的统一运维管理、安全策略维护及全网安全日志分析、消息中心、手机令牌、安全大屏、报表中心功能等。含≥50 点客户端功能授权，包括资产管理、防病毒、微隔离、账号风险检测、安全基线、漏洞防护、入侵监测、webshell 防护、系统防护、应用防护、网络防护等功能模块，含≥3 年使用授权。 2.支持 Windows Server 2003 sp2/R2 x86/x64、Windows Server 2008 sp1 及以上/R2 x86/x64、Windows Server

				2012~2019 sp1 及以上/R2 x86/x64、CentOs 5.0 及以上 x86/x64、RHEL 5.5 及以上 x86/x64、Ubuntu 14.04 及以上 x86/x64、SUSE 11 及以上版本 x86/x64 等操作系统。 3.所投产品需支持全量资产的关键字及语法搜索，支持检索的语法包括但不限于：服务器资产类、进程资产类、账号资产类、软件应用类、web 资产类、web 服务类、web 框架、数据库类、端口资产类、网络连接类、启动服务类、安装包类、计划任务类、环境变量类、内核类、类库资产类、注册表类、证书资产类进行检索。 4.所投产品需支持以列表的形式，统一列出 Windows/Linux 服务器的基础信息、离线服务器信息、硬件配置、进程资产、账户资产、软件应用资产、Web 站点资产、Web 服务资产、Web 框架资产、数据库资产、端口资产、启动服务或启动项、计划任务、环境变量、内核模块。对账号、端口、计划任务的变更进行监控，并显示变更的类型及变更内容。 5.所投产品需支持通过自动、手动的任务设置，对局域网内服务器的服务器进行扫描（支持 ARP、Ping、Nmap 扫描方式，并支持离线分析），并自动获取服务器相关信息，包括 MAC 地址、设备类型、未知主机 IP、操作系统、发现方式、首次发现时间等信息。 6.所投产品应支持以多种检测方式（RASP、内核监控、沙箱、内存 Webshell 等）检测 webshell 攻击。**（投标文件需提供能够体现上述功能配置选项截图复印件）** 7.产品应支持速度优先、性能优先两种 Webshell 扫描方式，且支持对多种文件类型进行扫描，包括但不限于 asa、asax、ascx、ashx、asp、aspx、cdx、cer、cgi、jsp、jspx、php、war、jpg、png、jpeg 等文件类型。**（投标文件需提供能够体现上述功能配置选项截图复印件）** 8.支持学习每台服务器的网络外连行为、命令执行行为、文件创建行为，并形成图形化的时间轴行为基线，对于偏离行为以外的动作进行告警。 9.所投产品需支持对一台或一组服务器进行白名单学习策略，并可设置学习时长，学习后可形成应用列表及 HASH 值，对偏离学习列表以外的应用进行告警和拦截。 10.★所投产品需支持设置端口的暴露控制规则，包括但不

				限于：禁止/允许外网暴露、禁止/允许内网暴露等策略，并支持例外端口的添加（**投标文件需提供能够体现上述功能配置选项截图复印件**）。 11.所投产品需支持对服务器的进程外连控制进行规则设置，包括但不限于：禁止/允许进程外连外网、禁止/允许进程外连内网，并支持进程白名单和例外进程的设置； 12.支持对主机进行一键隔离、一键禁止暴露外网、一键禁止暴露内网等快速应急操作； 13.所投产品需支持对服务器中的风险账户进行检测，发现可能存在的风险账号，并可对风险账号进行标记修复、加白等操作；支持对服务器中复用的相同密码进行检测，可识别出某个密码被哪些服务器、哪个账户、在什么操作系统上进行了复用。 14.所投产品需支持提供在漏洞检测功能基础上，开启虚拟补丁防护功能。虚拟补丁需与漏洞 CVE 编号关联，虚拟补丁防护可支持操作系统、web 服务器、中间件、数据库、应用等类型漏洞防护；（**投标文件需提供能够体现上述功能配置选项截图复印件**） 15.★所投产品需支持病毒实时防护功能，提供自主研发的病毒引擎，并支持用户在本地查杀、控制中心查杀、云查杀三种查杀模式灵活切换（**投标文件需提供能够体现上述功能配置选项截图复印件**）。 16.所投产品需支持实时监控服务器上发生的无文件攻击（漏洞型攻击、灰色工具型攻击、潜伏型攻击）事件，并对无文件攻击事件进行加白、标记处置等操作。 17.所投产品需支持 OOB 带外攻击检测，并支持黑域名的添加与同步。支持基于行为分析，检测对外服务的远程命令执行漏洞利用行为，实现实时告警和追溯 18.★所投产品需支持提供运行时应用自我保护功能。可提供 SQL 注入防护能力、XSS 防护能力且可自定义防护规则。（**投标文件需提供能够体现上述功能配置选项截图复印件**）。 19.所投产品需支持通过插件的方式，工作于 IIS、Apache、Nginx 等 web 中间件内部，通过判断流量特征和 WAF 规则引擎，对访问流量进行监控或防护，阻断 SQL 注入、XSS、漏洞利用等 Web 攻击。 20.所投产品需支持防端口扫描功能，且可设置单个 IP 请求

				时间范围、最大扫描端口数量、IP 锁定事件等信息；所投产品需支持微蜜罐功能，且可设置返回文本信息以及监听端口； 21.所投产品支持对系统防护、应用防护、网络防护、一键隔离等进行统一设置及模板管理，包括：文件监控与防护、入侵检测、应用高级防护、应用漏洞防护、虚拟补丁、防端口扫描等设置，并可将策略通过模板进行批量下发。 22.所投产品需支持对 Agent 进行统一管理，包括：Agent 降级，Agent 暂停，Agent 异常重启，Agent 安装的版本、可升级的版本占比情况进行统计，并可对 Agent 版本进行更新和同步，Agent 性能保护。 23.★可扩展支持对服务器的流量进行按需采集，将采集到的流量转发给本项目威胁监测分析系统进行分析。支持 VXLAN、GRE 转发协议，支持全量采集、按五元组过滤采集、自定义过滤采集三种采集规则。**（投标文件需提供能够体现上述功能配置选项截图复印件）**
9	威胁感知系统	套	1	**一、配置要求** 1.▲配置≥1 台分析平台。分析平台为标准 2U 机架式设备，配置≥4 个千兆电口，2*USB 接口；1*DB9 Console 接口，冗余电源；内存≥128G， ≥960G SSD+ 8*4TB 存储硬盘。处理能力≥10,000eps。含≥3 年威胁情报更新授权及产品维保服务。 2.▲配置≥3 台流量探针。流量探针为标准 2U 机架式设备，配置≥6 个千兆口，≥1TB 存储硬盘。系统吞吐量≥1Gbps，并发会话数 80W，新建会话数≥10000/s。含≥3 年威胁情报与检测引擎规则升级授权及产品维保服务。 **二、分析平台技术要求** 1.支持以分析平台为中心，可视化呈现设备的部署情况、运行情况、数据情况、联动情况。 2.支持以攻击者的维度进行分析，对攻击者进行画像，画像内容包括地理位置信息、国家信息、所属组织、使用的攻击手段、攻击的所有资产。 3.支持从威胁情报、应用安全、系统安全和设备安全的业务场景维度对告警进行攻击带外分析。 4.支持挖矿行为的分析，分析内容包括挖矿阶段、币种分布、挖矿告警趋势以及挖矿告警信息。 5.威胁情报维度分析包括：情报详情、影响资产列表、资产

				的行为（行为包含：DNS 解析、TCP 流量、UDP 流量、WEB 访问、文件传输）。 6.应用安全的细分维度包括：WEB 安全、数据库安全、中间件安全；系统安全的细分维度包括：暴力破解、弱口令、未授权访问、挖矿行为。 7.★支持与云端威胁情报中心联动，支持查看基本信息、相关样本、关联 URL、可视化分析、域名解析、注册信息、关联域名、数字证书等。可对攻击 IP、域名和恶意样本 MD5 进行一键搜索。**（投标文件需提供能够体现上述功能配置选项截图复印件）**。 8.支持对告警进行加白，加白参数包括：受害 IP（IP 段）、攻击 IP（IP 段）、威胁情报 IOC/规则 ID、威胁名称、XFF 代理、URI、域名、目的端口、源 IP（IP 段）、目的 IP（IP 段）、payload、referer。 9.支持可疑 DNS 解析：能够检测发现 DGA 域名与 DNS 隧道域名，支持根据时间范围、请求次数、DNS 域名总长度自定义 DNS 隧道检测规则。 10.支持远程工具分析：能够发现 pc_anywhere、ultra_vnc、chrome_remote_desktop、oray、teamviewer 等远程工具类型。 11.支持异常登录行为检测，检测内容包括：源 ip、账号、登录资产 IP、使用协议、登录结果等信息，且能进行异常时间配置。 12.支持对 mysql、mssql、oracle、sybase 等常见数据库高危操作行为分析，其能自定义规则。 13.支持外部访问分析，能展示源 ip、资产 ip、端口、协议、时间等详细信息，且能自定义源 ip 白名单。 14.支持风险端口访问分析，能自定义风险端口，且能自定义白名单。 15.支持对任意线索的自定义拓线及溯源取证分析，支持以可视化分析画布形式展示拓线过程并支持结果快照导出；支持对于给定线索的溯源结果展示，包括但不限于攻击溯源、失陷主机分析、暴力破解分析、弱口令分析等。 16.支持告警日志检索，可基于时间、告警类型、文件 MD5、文件名、文件传输方向、攻击方式、攻击结果、来源/目的所属国、IP 地址、上下行负载等多字段混合搜索。

				17.支持大屏展示网络攻击态势，包括整体网络风险指数、告警总数、攻击次数、攻击 IP 数、攻击源国家/地区 TOP5、攻击态势，并支持自动翻转的攻击全景地图展示。 18.支持大屏展示外部访问态势，包含外部 IP 访问次数 TOP5、资产被访问次数、访问趋势图、可视化地图炮。 19.支持大屏展示整体资产风险态势，包含资产矩形树结构、资产分类、资产概况、开放服务统计、资产风险状态。 20.★支持工作流程自定义编排，支持联动服务管理，支持 python 语言与 javascript 语言在 web 页面编辑联动服务（**投标文件需提供能够体现上述功能配置选项截图复印件**）。 21.支持编排处置日志记录，记录处置时间、受害 ip、攻击 ip、告警类型、威胁名称、域名、处置策略、告警来源等信息。 22.支持分析平台横向扩展至多台设备集群。 23.告警联动配置：支持通过飞书和钉钉进行告警通知；（**投标文件需提供能够体现上述功能配置选项截图复印件**） 24.支持与本项目终端安全管理系统进行联动，发现威胁事件后支持与控制中心进行指令下发执行终端隔离和扫描操作； 25.支持与本项目网络准入认证系统进行联动，发现威胁事件后支持与控制中心进行指令下发执行阻断操作； 26.▲**支持与本项目出口防火墙、数据中心防火墙进行联动，发现威胁事件后支持对攻击 IP、恶意域名和受害资产的流量进行阻断（将策略下发给防火墙，由防火墙执行阻断）** 27.★支持与本项目服务器安全管理系统联动，扫描弱口令、主动隔离失陷主机。（**投标文件需提供能够体现上述功能配置选项截图复印件**） 28.为提升医院对未知威胁的快速处置能力，要求威胁感知系统支持基于入侵检测规则、威胁情报的旁路阻断功能。支持根据时间段、IP、域名等条件配置阻断黑名单、阻断白名单。支持配置观察模式，仅记录不阻断。 **三、流量探针技术要求** 1.支持常见协议识别并还原网络流量，用于取证分析、威胁发现，支持：http、dns、smtp、pop3、imap、webmail、DB2、Oracle、MySQL、sql server、Sybase、SMB、FTP、SNMP、telnet、nfs、ICMP、SSL、SSH 等。 2.支持 TCP/UDP 会话记录、异常流量会话记录、web 访问

				记录、域名解析、SQL 访问记录、邮件行为、登录情况、文件传输、FTP 控制通道、SSL 加密协商、telnet 行为、IM 通信等行为描述。 3.支持自定义协议和端口，满足特殊场景下的流量抓取。 4.支持基于流量实时 IOC 匹配功能，设备具备主流的 IOC，情报总量 550+万条。 5.★支持基于工具特征的 WEBSHELL 检测，能发现威胁如：中国菜刀、小马上传工具、小马生成器等（**投标文件需提供能够体现上述功能配置选项截图复印件**）。 6.支持基于代理程序的攻击检测，如 TCP 代理程序、HTTP 代理程序等。 7.支持与云端威胁情报中心联动，可对受害 IP、攻击 IP、IOC/规则 ID、文件 MD5 进行一键搜索，查看基本信息、开源情报、相关样本、可视化分析、域名解析、注册信息、关联域名、数字证书等。 8.支持基于网络请求的语义分析检测，能够将网络请求拆分后从请求头、响应头、请求体、响应体四方面详细展示请求内容，提升对未知威胁检测能力。 9.支持攻击特征高亮展示，方便分析人员事件分析。 10.支持自定义弱口令字典，支持 HTTP、HTTPS、Telnet、FTP、POP、SMTP、IMAP 等协议的自定义弱口令检测。 11.★针对流量中的威胁，支持基于 IP 和域名的的旁路阻断。支持自定义生效时长、将请求重定向至指定 IP、域名；（**投标文件需提供能够体现上述功能配置选项截图复印件**） 12.支持扩展高级威胁旁路阻断功能，支持基于威胁检测规则，适用规则不少于 2000 条；（**投标文件需提供能够体现上述功能配置选项截图复印件**） 13.支持根据攻击载荷自定义漏洞检测规则，可自定义载荷检测位置、检测字段、匹配方式（文本匹配/正则匹配）、匹配载荷内容，并且单条规则可指定多个检查项，同时可定义漏洞威胁级别、威胁分类、攻击结果、CVE 编号、CNNVD 编号、漏洞描述、漏洞危害、解决方案。 14.支持根据威胁类型、威胁名称、情报类型、IP 自定义威胁情报。 15.支持 AES256、SM4 数据传输加密，确保数据传输的安

				全性。 16.★支持旁路 HTTPS 解密进行威胁检测（**投标文件需提供能够体现上述功能配置选项截图复印件**）。 17.支持将威胁告警外发集中管理平台，支持与集中管理平台进行联动，统一进行系统、情报、规则的升级。
10	网页防篡改	套	1	1.支持防篡改管理中心通过统一的管理中心进行远程管理、策略下发和日志收集，配置≥10 个网站目录防篡改客户端，支持 Windows、linux 等主流操作系统网站，含≥3 年维保服务； 2.支持提供自我保护机制，网页防篡改客户端需有第三方认证码方可卸载； 3.支持采用基于文件过滤驱动保护技术、事件触发机制相结合方式的网页防篡改功能； 4.支持防护模式和监控模式两种模式的防篡改模式； 5.支持在断线情况下对网页文件目录的防护功能； 6.支持文件多线程同步，并可以设置文件空闲同步时间周期、发布时间周期等设置； 7.支持网页防篡改异构同步(linux 与 Windows 双平台)，支持管理中心将 Windows 平台及 Linux 平台的防护端和发布端混用，同步都能够正常进行； 8.支持服务器网站异常检测(linux 与 windows 双平台)，检测防护端所在服务器网站进程是否正常或存在 9.支持网页防篡改支持增加策略生效时间控制，可在防护端设置防篡改功能的启用与停用的时间 10.支持防篡改插件安装时不重启 Web 服务器；支持 IIS、Weblogic、Websphere、Apache、Tomcat 等 Web 服务器；
11	漏洞扫描系统	台	1	**一、配置要求** 1.机架式设备高度≥1U，硬盘≥1T；配置不少于 4 个以太网千兆电口，不少于 4 个千兆以太光接口，不少于 1 个管理口。 2.系统扫描最大可扫描 IP 数量≥256，系统漏扫并发任务数为≥5，单任务系统扫描最大并发扫描 IP 数为≥120，弱口令扫描并发任务数为≥1； **二、技术参数要求** 1.支持多路扫描功能，设备所有网口均可用于扫描，支持同时对多个隔离子网进行扫描。 2.网络配置需提供快速配置向导，支持快速部署上线。

				3.支持自适应网络扫描，根据网络状况自动控制发包速率，避免影响用户网络。 4.支持针对工控专用设备包括 PLC、SCADA、DCS、工控专用网络设备的漏洞扫描，支持扫描的工控插件不少于 300 条。 5.支持目前主流协议和数据库弱口令检测，包括：TELNET、FTP、SSH、POP3、SMB、SNMP、RDP、SMTP、Tomcat 、Oracle 、 REDIS 、 MySQL 、 PostgreSQL 、 MsSQL 、 DB2 、MongoDB、Sybase 、Informix。 6.支持漏洞数据高级检索及分析，支持按照目标 IP 或 URL、操作系统、MAC 地址、资产评分、漏洞等级、漏洞名称、漏洞类别、漏洞评分、开放端口查看漏洞分布情况，并将检索结果导出。 7.漏洞库支持在线升级、FTP 方式升级、本地导入升级，在线升级支持设置周期自动升级时间，支持通过代理方式进行升级。 8.支持导出同时包含系统扫描、Web 扫描、弱口令扫描结果的报表，可以统一分析网站漏洞、网站所在主机漏洞以及主机弱口令。 9.支持检测的漏洞数大于 65000 条以上，涵盖漏洞标准包含 CVE、CVSS、CNVD、CNNVD、CNCVE、Bugtraq6 种，CVSS 覆盖 CVSS2 和 CVSS3 版本。 10.支持自带诊断工具，包含 PING、WGET、端口探测、Tcpdump 抓包、故障信息收集、一键诊断修复等工具。
12	数据库审计系统	台	1	**一、性能要求** 1.配置不少于 8 个以太网千兆电口，不少于 6 个以太网千兆光口。配置交流冗余电源，≥4T SATA 硬盘。 2.SQL 峰值处理能力≥35000 条/秒，数据库吞吐量≥300Mbps，支持数据库版本数量≥4。 **二、功能参数** 1.支持主流数据库：Oracle，SQLServer，MySQL、DB2、Sybase、Informix、PostgreSQL、HBase、MongoDB、DM、kingbase、OSCAR、Gbase、Hive、Redis、Cache、Highgo、MariaDB、Teradata、ElasticSearch 2.支持多种部署方式：支持旁路镜像与 Agent 同时部署的混合部署方式；支持分布式部署，管理中心可实现统一配置、统一

				报表生成、统一查询； 3.支持在 IPV4 环境中部署，且支持所有数据库 IPV4 协议的审计。支持在 IPV6 环境中部署，且支持所有数据库 IPV6 协议的审计； 4.支持数据库自动发现，设备无需添加、即插即用。 5.系统能对基于数据库漏洞进行攻击行为监测和告警，默认支持 400 个以上的数据库漏洞攻击规则库。 6.支持数据库请求和返回的双向审计，包含：会话的终端信息、会话的主机信息、操作等信息，支持通过返回行数和内容大小控制返回结果集大小。 7.支持 MySQL 数据库的 SSL/TSL 加密链路审计。 8.系统可审计到执行人、执行内容、执行时间、执行地点、执行方式、影响范围以及执行结等内容。 9.针对高风险数据库操作所在的会话，支持旁路阻断功能，且支持阻断时间自定义，避免更大的危害。 10.可以通过模式匹配的方式对 SQL 访问进行监测与告警，判断是否为可疑 SQL 注入，提供 SQL 注入特征库。 11.支持风险语句告警策略，支持自定义添加风险语句和可信语句。 12.支持手动创建规则模板，规则类型需包含：口令攻击、SQL 注入、账号滥用、访问规则、风险操作等；支持规则模板的手动导入导出。 13.根据不同的安全级别采用不同的响应方式，包括记录、告警；告警方式包括：邮件、短信、SYSLOG、SNMP、FTP、企业微信、钉钉等。 14.为保证系统自身安全，系统应支持系统管理员、安全管理员和审计管理员等三权分立的用户身份验证。
13	负载均衡	台	2	**一、配置要求** 1.采用专用多核硬件架构，机架式设备高度≥1U，交流冗余电源。配置不少于 10 个千兆电口，不少于 8 个千兆光口，不少于 8 个万兆光口；支持不少于 3 个接口扩展槽。配置≥480GB SSD 硬盘。配置 2 个万兆多模光模块。 2.整机吞吐量≥20G，L4 新建连接数≥12 万，并发连接数≥1000 万。 **二、技术参数要求**

				1.支持端口聚合，支持静态模式以及 LACP 模式。 2.支持 Vlan、QinQ、STP、MSTP 等二层协议，满足二层的区域隔离以及链路冗余。 3.支持多种链路检测方法，能够通过 ICMP、UDP、TCP、FTP、DNS、HTTP、RADIUS、SSL、HTTPS、TCP half-open、SNMP-DCA、RADIUS-ACCOUNT 等方式监控链路的连通性。 4.支持以下协议的 ALG 功能，包括但不限于 DNS、RTSP、PPTP、SCCP、XDMCP、FTP、RSH、NBT、SCCP、H323、SQLNET、MGCP、SCTP、SIP。 5.支持 RIP、OSPF、BGP 等路由协议以及各自的 IPv6 版本。。 6.支持基于 ToS、五元组条件（源 IP 地址，源端口，目的 IP 地址，目的端口，传输层协议号）来配置出站访问的链路调度策略。 7.支持 DDNS，动态更新 DNS 服务器上域名和 IP 地址之间的对应关系，保证通过域名解析到正确的 IP 地址。 8.支持 CARP 算法，在不借助会话保持的前提下，当服务池中的某个服务器故障时，只有故障服务器上的业务流量重新 HASH 调度，正常服务器上负载的业务不重新进行 HASH，将业务系统的震荡降到最低。 9.支持多个 PPPoE 出口的链路负载。 10.支持基于加权 HASH 算法、最快响应算法，以达到更灵活的算法控制。 11.通过 ICMP、TCP、DNS 等方式，检验 SNAT 地址池中的地址有效性，避免出口 SNAT 池中地址被意外封杀后仍然被使用造成网络访问中断。
14	外网核心交换机	台	1	1.采用正交 CLOS 结构设计，总槽位数≥9 个，独立业务槽位数≥6 个，独立交换网板槽位数≥1 个； 2.交换容量≥230Tbps，包转发率≥72000Mpps；配置双主控引擎双电源； 3.配置不少于 4 个 100G 光接口（向下兼容 40G），不少于 24 个 25G 光接口（向下兼容 10G），不少于 8 个万兆以太网光接口，不少于 48 个千兆电口，不少于 40 个千兆光接口；配置不少于 10 个万兆多模光模块，不少于 4 个 40G 多模光模块； 4.支持主控、网板、风扇、电源、光模块热插拔。

				5.支持防火墙/应用控制网关/流量分析/无线控制等安全板卡。 6.支持流量管理，支持基于 802.1p 和 ToS 的 Qos 带宽控制，支持 MQC 的 Remark 动作，支持流量整形 Shapping。 7.支持 INQA（IPCA）功能，通过直接对业务报文进行标记的方法，实现对网络级和设备级的丢包统计。 8.支持将多台高端设备虚拟化为一台逻辑设备。 9.支持 IPv4/IPv6 双协议栈，支持多种隧道技术，支持 IPv4/IPv6 等价路由，支持 IPv4/IPv6 的组播技术。 10.支持硬件级加密技术 Macsec 技术（802.1ae），区别于传统端到端基础应用层保护的软加密技术，Macsec 通过鉴别数据源的密码技术保护管理桥接网络和其他数据的控制协议，保护信息完整并提供再保护和保密服务。 11.支持内置智能管理功能，支持通过图形化界面设备配置及命令一键下发和版本智能升级。 12.支持 M-LAG 跨设备链路聚合技术(原 DRNI 技术)，通过将两台物理设备在转发层面虚拟成一台设备来实现跨设备链路聚合，保持控制层面互相独立，从而将单板级可靠性提升至设备级可靠性。
15	网闸	台	2	1.★应用层吞吐≥5Gbps，应用层并发连接≥15 万条。2U 机箱，冗余电源，支持液晶面板，内外网分别配置 1 块 256GB SSD 固态硬盘存储。内网接口：≥6 个 10/100/1000Base-T 端口，≥4 个 SFP 插槽, ≥2 个 SFP+插槽，1 个 Console 口，2 个 USB 口，支持 1 个扩展槽位。外网接口：≥6 个 10/100/1000Base-T 端口，≥4 个 SFP 插槽, ≥2 个 SFP+插槽，1 个 Console 口，2 个 USB 口，支持 1 个扩展槽位。提供≥3 年维保服务。 2.★采用“2+1”模块结构设计，即包括外网主机模块、内网主机模块和隔离交换模块，内外端机为网络协议终点，彻底阻断各种网络协议；产品包含文件交换、数据库同步、数据库访问、邮件访问、安全 FTP、安全浏览、定制模块、工控模块、视频模块、SSL 通道、双机负载、日志审计、告警中心、防病毒等全功能模块，所有模块功能开启； 3.支持双系统冗余架构，可通过 WEB 页面进行主备系统切换，当主系统发生故障或需要升级时可切换至备系统进行工作。 4.内、外网主机分别具有独立液晶屏，能够显示产品品牌、

				型号、CPU/内存占用率、网络接口状态等信息。 5.文件交换支持传送优先级，可根据文件大小、新旧、文件名、后缀、缓时传输等多种方式进行优先级排序传输。 6.★支持实时监控文件同步进度、当前同步文件大小、已传输大小、花费时长、同步速率**（投标文件需提供能够体现上述功能配置选项截图复印件）**。 7.文件传输具备文件名过滤、文件类型过滤、文件内容过滤、文档重建、病毒过滤**（投标文件需提供能够体现上述功能配置选项截图复印件）。** 8.支持文件重构技术，可自动剔除文件中夹带的危险程序，可执行代码等； 9.★同时支持文件并发数量设置，大幅度提升文件传输性能，充分利用硬件资源；**（投标文件需提供能够体现上述功能配置选项截图复印件）。** 10.数据库同步可指定资源使用情况，按照任务优先级进行资源分配，可灵活设置一个或者一组任务所使用最小内存、最大内容等资源情况。 11.为保障医院数据库数据同步安全，要求网闸具备数据库数据防泄漏能力，可对数据库字段进行敏感信息脱敏过滤，支持正则表达式、关键字、枚举、数值区间、时间区间等方式来匹配关键字段内容，支持替换成指定内容进行数据脱敏。 12.数据库同步支持无客户端方式同步，无客户端方式同步由网闸主动发起并完成，不需要第三方软件支持（无需在数据库安全任何第三方软件，可以在网闸系统上完成数据库同步配置）。 13.支持文件和数据库的异构同步，满足将 XML、Excel、CSV 类型文件内容同步至数据库中，或将数据库内容同步至 XML、Excel、csV 类型文件中。 14.★支持云查杀模式，预判文件安全风险，防止恶意文件通过网闸进入内网，提供高中低不同级别阻断策略**（投标文件需提供能够体现上述功能配置选项截图复印件）。** 15.支持数据库库名控制、数据库表控制，可以根据用户与数据库表对应关系，进行相应数据库操作过滤。 16.安全 FTP 支持最大并发连接数、单个 IP 最大并发数设置，灵活限制数据库通道是否在 1024 以下端口使用。 17.支持安全审计能力，可通过自定义时间、任务名称、文

				件名称、文件类型、文件大小类型、源目的文件路径、源目 IP 等详细字段追溯业务数据流向，可自定义配置查询条件，查询条件策略可以自定义设置。 18.支持 FTP、SFTP、SMB、NFS 等协议进行日志导出到指定服务器目录下。
16	上网行为管理系统	台	2	**一、性能参数** 1.网络层吞吐量≥10Gbps，带宽性能≥1Gbps，并发连接数≥60W，新建连接数 1.2W，支持用户数 6000。 2.1U 规格。标配≥6 个千兆电口，≥2 个万兆光口，存储不少于 1TB。 **二、功能参数：** 1.为保障设备高可靠性能，必须支持两台及两台以上设备同时做主机的部署模式。 2.为满足 IPv6 改造需求，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。 3.为提高运维管理效率，降低运维难度，需要提供图形化排障工具，便于管理员排查策略错误等故障。 4.为提高运维管理效率，密码登录支持用户自注册，通过 Web 页面申请注册新账号，管理员审批后新账号可用，自注册同时支持 portal 认证和 802.1x 认证。 5.为提高采购人使用体验，支持 DNS 透明代理，能够基于用户、域名、目标 DNS，指定代理策略生效，代理策略可以设置为：重定向至 DNS 服务器、解析为 IP、丢弃、重定向至指定线路。 6.为便于内部人员快速上线和投入使用，需要支持 IPsec VPN 支持与 LDAP 服务器、Radius 服务器结合认证。 7.为便于及时掌握网内情况及问题排查，需要支持查看当前设备的线路状态，线路带宽利用率以及当前策略的引流流量分布和实时的引流策略，支持下钻设置线路流控策略。 8.为帮助及时掌握用户 WEB 访问质量，需支持针对内网用户的 web 访问质量进行检测，对整体网络提供清晰的整体网络质量评级；支持以列表形式展示访问质量差的用户名单；支持对单用户进行定向 web 访问质量检测。 9.为保障用户使用体验，需支持通过 OAuth 认证协议对接，

				支持阿里钉钉，口袋助理，企业微信第三方账号授权认证，支持企业微信、口袋助理、钉钉 这三个平台支持同步组织结构，用户通过企业微信、口袋助理、钉钉认证上线，本地会创建与认证服务器上对应的用户组，用户会上线到对应创建的组。 10.为提高系统易用性，需支持 radius、AD、POP3、Proxy、PPPOE、 H3C IMC/CAMS、锐捷 SAM、城市热点等系统进行认证单点登录，简化用户操作，可强制指定用户、指定 IP 段的用户必须使用单点登录。 11.为提高安全性同时保障员工使用体验，需要能够对新浪微博、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。 12.为提升网络安全性，需支持基于 802.1x 的外部 CA 证书认证，同时支持在线证书状态查询（OCSP）。 13.为降低运维人员运维压力，需支持以图表方式显示移动终端接入趋势。 14.为协助网络内资产梳理，需支持自动发现网络里面的终端，并获取 IP、Mac、厂商、操作系统、开放服务、开放端口等信息，设备必须支持 PC、移动设备、哑终端、专用设备的发现和型号识别：至少支持 Windows、Linux、MAC、瘦客户机等 PC；至少支持手机、平板等移动设备；至少支持服务器、交换机、无线控制器等 7 类网络设备；至少支持打印机、投影仪、电视、摄像头、门禁系统等 10 类哑终端。 15.为帮助了解内部人员审计情况，需要支持首页分析显示接入用户人数、终端类型、认证方式；资产类型分布、新设备发现趋势、终端违规检查项排行、终端违规用户排行；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。
17	零信任（可信访问控制台）	台	1	1.★2U 高度，冗余电源，配置≧2 个千兆电口，3 个扩展槽，4 个 USB 接口，对外提供 1 个千兆 RJ45 管理网口；最大支持并发用户数（个）≧1800；配置不少于 200 个并发授权，不少于 200 个双因素认证授权；含≥3 年质保。 2.支持 UDP+TCP 单包授权机制，UDP+TCP 方式默认不开放端口，可避免业务应用的端口被扫描，进而避免利用端口对业务应用发起攻击的风险。 3.支持通过输入安全码激活客户端，完成 SPA 敲门。安全

				码可支持共享码、一人一码两种模式。 4.提供用户概览统计能力，包括用户总数、启用用户数、锁定用户数、禁用用户数等信息，提升管理员运维能力。**（投标文件需提供能够体现上述功能配置选项截图复印件）** 5.支持用户身份属性的自定义扩展，以便管理员可以根据自身需要对用户属性扩展，而不需要重新部署或升级系统程序。 6.支持用户身份打标签，以实现对不同的用户打不同标签，并可以基于标签进行细腻度访问控制。 7.★提供设备概览统计能力，包括终端总数、启用终端数、锁定终端数、禁用终端数等信息。提供设备绑定概览统计能力，包括绑定总数、管理员绑定数、申请绑定数、自助绑定数等信息，提升管理员运维能力。**（投标文件需提供能够体现上述功能配置选项截图复印件）** 8.支持设备审批概览统计能力，管理员能够明确知道总数、待审批数、已通过数、已驳回数等信息。 9.支持 PC 端发起访问应用的采集，能够对应用进行标记为可信或不可信，可用于访问控制策略，从而实现基于访问进程的细粒度控制措施。 10.支持 MacOS 操作系统终端环境感知功能，可针对高危端口、开启屏幕共享、开启文件共享、开启互联网共享、开启蓝牙共享、开启打印机共享、开启内容缓存、开启远程管理，开启远程登录，开启防火墙，开启远程 APPLE 事件等环境感知和采集，以实现基于 MacOS 终端安全状况的访问控制措施。 11.支持移动端环境感知功能，可针对操作系统版本、设备 ID、系统是否被 ROOT/越狱、USB 调试模式开启、锁屏密码开启、蓝牙开启、NFC 开启、WiFi 热点开启、自动填充服务开启等环境感知和采集，以实现基于移动终端安全状况的访问控制措施。 12.支持 UOS、Kylin、Linux 端操高危端口、运行的软件、零信任客户端版本、运行的杀毒软件、运行的远控软件、运行的虚拟机软件、安装的防病毒软件等环境感知和采集，以实现基于终端安全状况的访问控制措施。 13.支持应用概览统计能力，包括应用总数、WEB 应用数、隧道应用数等信息，提升管理员的运维能力。 14.支持 WEB 应用支持数据传递，可通过 URL、Header、

				Cookie 自定参数传递，以满足应用对特定参数的需要，从而实现对现网应用无需修改即可正常访问。 15.支持移动端集成的配置，以便通过 SDK 与安全访问系统集成。 16.支持设备认证，提供认证策略配置，可根据是否签发设备、导入设备、绑定设备进行设备认证。 17.★权限管理：支持从应用资源选择用户、组织机构、用户组，方便管理员进行权限配置，提升运维水平。**（投标文件需提供能够体现上述功能配置选项截图复印件）。** 18. 可针对 Windows、macOS、Android、IOS 以及 UOS/Kylin/Linux 终端操作系统设置准入策略，支持从用户属性、环境属性、行为属性、终端属性维度设置，便于对用户准入进行控制。 19. 可针对 Windows、macOS、Android、IOS 以及 UOS/Kylin/Linux 终端操作系统设置动态访问控制，支持从环境属性、应用属性、用户属性、终端属性维度设置，便于对用户访问资源进行控制。 20.★支持应用限流限速功能，支持通过限制请求并发设置阈值、通过限制请求速度来设置阈值、通过限制单位时间内的请求数设置阈值、限制响应传输速率设置阈值、通过限制请求大小设置阈值。**（投标文件需提供能够体现上述功能配置选项截图复印件）**。 21.支持与本项目终端安全管理系统联动，零信任可以支持联动终端安全管理系统登录上线、终端安全可以联动安装零信任客户端、终端安全管理系统可以集成零信任客户端入口。 22.为提升系统安全，要求零信任系统支持与本项目服务器安全管理系统联动，实现更加安全的自身防护能力。
18	零信任（可信应用代理）	台	1	1.★2U 高度，冗余电源；配置不少于 4 个千兆电口，2 个扩展槽，1 个 MGT 口，1 个 HA 口；加密流量支持≧480 Mbps，并发用户数支持≧1600 个，HTTPS 并发连接数≧48000 个/秒；≥3 年质保； 2.可信应用代理需要与可信访问控制平台配合使用，需要与可信访问控制平台为同一品牌。 3.支持 TCP 单包授权机制；支持 UDP+TCP 单包授权机制，UDP+TCP 方式默认不开放端口，可避免业务应用的端口被扫

				描，进而避免利用端口对业务应用发起攻击的风险 4.管理 TLS 加解密算法的强度，支持国际商密算法会话协商：AES128-SHA,AES256-SHA,ECDHE-RSA-AES128-GCM-SHA256,ECDHE-RSA-AES256-GCM-SHA384,ECDHE-RSA-AES128-SHA,ECDHE-RSA-AES256-SHA,DES-CBC3-SHA,RC4-SHA,RC4-MD5。 5.支持接入国密卡和国密算法：支持 ECC-SM4-SM3 算法，以满足对国密合规性要求。 6.★支持预防 synflood 攻击、忽略 icmp 回显请求以及通过 TOA 识别源。**（投标文件需提供能够体现上述功能配置选项截图复印件）** 7.支持系统时间配置，可设置时区，支持手工、NTP 服务器方式同步时间。 8.★支持应用代理的 Ajax 请求响应选项、请求头大小限制、响应头大小限制等。**（投标文件需提供能够体现上述功能配置选项截图复印件）** 9.支持连接到访问控制台，并根据访问控制台的自身策略，提供文件监控与防护，可监控与防护文件的读取、写入、删除、创建、执行、链接、重命名操作，从而缓解通过恶意文件的方式，对零信任系统进行攻击的安全风险。 10.支持连接到访问控制台，并根据访问控制台的自身策略，提供暴力破解防护，支持在 2 分钟内同一 IP 错误登陆 SSH 后台 10 次，该 IP 将被锁定 1 小时，从而缓解暴力攻击尝试登录管理后台，对安全访问系统进行攻击的安全风险。 11.★支持逃生模式，当控制中心故障时不进行权限处置对业务访问进行放行。**（投标文件需提供能够体现上述功能配置选项截图复印件）**
19	边界防火墙	台	2	1.标准 2U 设备，冗余电源；配置不少于 14 个 10/100/1000M 自适应电口、不少于 4 个千兆光口、不少于 4 个万兆光口，另有不少于 2 个接口板卡扩展插槽，1 个 Console 口，具备液晶屏，≥256GB SSD 硬盘。含≥3 年硬件质保。 2.防火墙吞吐≥20Gbps，并发连接数≥500 万，每秒新建连接数≥15 万/秒，包含应用控制、URL 过滤、病毒防护、入侵防御、威胁情报检测等功能模块。配置≥3 年防病毒、入侵防御特

				征库升级服务 3.所投产品支持 MPLS 流量透传；支持针对 MPLS 流量的安全审查，包括漏洞防护、反病毒、间谍软件防护、内容过滤、URL 过滤、基于终端状态访问控制等安全防护功能。 4.所投产品支持基于策略的路由负载，支持根据应用和服务进行智能选路，支持源地址目的地址哈希、源地址哈希、轮询、时延负载、备份、随机、流量均衡、源地址轮询等路由负载均衡方式。 5.所投产品支持在源地址转换过程中，对 NAT（源地址转换）使用的地址池利用率进行监控，并在地址池利用率超过阈值时，通过 SNMP Trap、邮件等方式告警。 6.所投产品支持 DDNS 功能，支持 Oray 向日葵、Pubyun 公云、Noip、Changeip 提供的 DDNS 服务，将动态获取的 IP 地址映射为固定的域名。 7.所投产品支持 DS-Lite CPE B4 功能，支持成为 b4 或 aftr 角色，支持从 DHCPv6 服务器或手动方式获取 AFTR 参数。 8.所投产品支持在虚拟系统内独立配置病毒防护、漏洞利用防护、间谍软件防护、URL 过滤、文件过滤、内容过滤、邮件过滤、行为管控等安全功能。并可支持对本虚系统内产生的日志进行独立审计。 9.所投产品支持基于源安全域、目的安全域、源用户、源地址、源地区、目的地址、目的地区、服务、应用、隧道、时间、VLAN 等多种方式进行访问控制，并支持地理区域对象的导入以及重复策略的检查。 10.所投产品支持共享上网检测功能，可以通过设置管控地址和例外地址优化管控功能，同时支持阻断或告警动作。 11.所投产品支持将其他硬件安全设备（包括但不限于防火墙、IPS、IDS、WAF、行为管理、流量探针等）加入网元组，并接受流量编排；支持将同类型安全设备划归同一网元组，组成硬件安全资源池（如 WAF 安全资源池），并将流量通过负载均衡（“源地址哈希”、“源目的地址哈希”，“加权源地址哈希”、“加权源目的地址哈希”、“加权地址端口哈希”、“轮询”和“权重轮询”）的方法编排给组内所有网元。 12.所投产品支持灵活的服务链编排功能，支持串接链和旁路链，支持网元组的方向和位置设置。

				13.所投产品支持灵活的细粒度引流策略，可基于源安全域、目的安全域、源用户、源地址、目的地址、服务、VLAN、服务链、流量方向（内网到外网/外网到内网）的引流策略，并详细记录日志。 14.所投产品支持对编排的流量进行监控，至少能从网元组、引流策略两个维度对编排流量监控统计。 15.所投产品支持基于不同安全区域防御 SYN Flood、UDP Flood、ICMP Flood、IP Flood、DNS Flood、HTTP Flood、NTP Query Flood 、NTP Reply Flood 和 SIP Flood 攻击，并支持警告、丢弃、普通防护（首包丢弃）、增强防护（TC 反弹技术）、授权服务器防护（NS 重定向）、普通防护（自动重定向）、增强防护（手工确认）等多种防护措施。 16.所投产品支持 DHCP 协议防护；支持手动定义可信 DHCP 服务器 IPv4 和基于阈值限制 DHCP 请求传输速率。 17.所投产品支持 IPv4 和 IPv6 流量的 HTTPS、POP3S、SMTPS、IMAPS 协议进行解密，支持配置基于源安全域、目的安全域、源地址、目的地址、SSL 协议服务的解密策略，动作可以设置解密或不解密。 18.所投产品支持 IPv4 和 IPv6 流量的蜜罐引流策略，支持配置基于源安全域、目的安全域、源地址、目的地址、服务、VLAN 的引流策略，并支持强制导流，能够通过设置服务器和端口进行引流。**（投标文件需提供能够体现上述功能配置选项截图复印件）** 19.所投产品支持资产管理，能够通过设置资产监控、VPN、源安全域来控制资产识别范围，支持 scanner 或 onvif 类型的扫描方式和网段，实现自动或手动资产扫描；支持通过设置 IP 地址、MAC 地址、资产类型、生效市场、厂商、位置等信息来制定黑/白名单，方便日常资产管理。 20.具备 LLDP 功能，可以向网络中其它节点公告自身的存在，并保存各个邻近设备的发现信息，如设备配置和设备识别等详细信息。
20	远程安全运营服务	项	1	**1.▲通过云端安全团队"专人专岗""7x24 小时"持续保障，针对各类威胁事件进行实时告警监测、深度分析、应急处置的完整闭环响应，帮助采购人及时感知安全威胁事件，及早采取预防措施，降低可能造成的影响，最大限度避免客户的安全损失。安全运营服务（含 7×24 SLA 响应资产（IP）监控数量≥20 个），**

				服务期限≥3 年； **2.资产管理** （1）设备管理和维护：为保障设备正常运转，服务人员每日巡检流量采集状况、存储情况、授权、规则和情报更新状态等，避免故障和异常影响设备威胁检测能力。为保障设备安全监测能力，服务人员定期对设备进行威胁情报、规则库进行更新，对系统进行版本升级。为保障云端运营平台及服务工具正常运转，日常巡检发现设备故障后，服务人员协调跟踪产品售后人员对设备进行故障修复。 （2）服务资产管理：提供安全托管中心资产管理模块，每季度协助客户更新监测资产的台账，通过安全托管中心，提供告警、资产关联分析能力。 **3.漏洞管理** （1）持续漏洞利用情况监测：利用云端安全运营平台持续监测客户处漏洞利用情况，对监测发现的安全漏洞进行验证分析和跟踪整改情况。 （2）资产漏洞预警：结合漏洞监测平台信息，通过沟通群对客户资产漏洞进行预警。 （3）漏洞修复指导：对监测发现的客户处漏洞进行分析，提供可落地专业漏洞修复指导。 （4）漏洞确认：对用户服务内资产，监测发现的漏洞远程进行研判确认。 **4.威胁管理** （1）流量威胁检测：提供威胁检测响应工具，对网络内流量进行检测，包括网页漏洞利用情况检测、网络攻击检测、webshell 检测、威胁情报检测（APT、恶意软件）等。 7*24 安全威胁监测：服务人员通过云端托管运营平台提供 7*24 安全威胁监测服务，持续监测网络内的安全隐患情况并进行分析，包括对外部网络攻击网络漏洞利用情况、恶意软件活动情况、以及内网安全情况。 （2）主动响应分析：服务人员综合所发现的安全事件、攻击情况，评价客户侧整体网络安全态势，包括但不限于告警趋势分析、威胁类型分布分析、安全事件分析等。 **5.事件管理** （1）安全事件通告：服务人员对安全监测发现的安全隐患

				及事件在服务规定时间内进行通告，同时根据客户需求每日同步安全情况。 （2）威胁抑制/阻断：建立工作群，实时推送封禁信息，包括高频攻击源、恶意软件 IOC、内外交互的恶意链接等。安全运营平台可联动同品牌防火墙、终端安全管理产品，进行联动封禁，阻止进一步攻击。 （3）入侵影响抑制：通过事件检测分析，提供抑制手段，降低入侵影响，协助快速恢复业务 （4）事件跟踪管理：提供安全托管中心-工单管理模块，对事件处置过程进行跟踪形成闭环，在实战中不断加固，协助推动用户建立可行的事件处置流程。 **6.运营汇报管理** （1）运营汇报及解读：安排资深专家在线进行运营情况汇报，进行威胁分析情况解读，并进行疑难解答。 （2）安全运营问题解答：通过沟通群等对安全运营中的产品问题、安全分析问题进行解答，协助进行问题解决。 **7.服务交付物** （1）《服务启动会 PPT》 （2）《首次分析报告》 （3）《事件报告》 （4）《服务周报》（按需） （5）《服务月报》 （6）《漏洞修复指导》（按需） （7）《漏洞预警报告》（按需） （8）《总结汇报 PPT》等。
21	网站云监测服务	项	1	1.提供≥5 个域名≥3 年网站云监测平台的使用权。提供漏洞扫描、违规内容监测、网页挂马监测、内容变更监测、黑链监测、网站可用性监测、标准的报表管理和通报管理模块。提供 7X24 小时的安全事件监测验证和安全事件通告下发、远程漏洞扫描及高危漏洞人工验证 7X24 小时电话售后服务。 2.系统基于云架构，无需用户部署任何软硬件，通过账号可以直接进行管理。 3.每日扫描网站一万个以上，扫描深度最高可达 9999。 4.对发现网站存在的 SQL 注入、XSS 跨站脚本、目录遍历、文件包含、备份文件、敏感文件等漏洞，检测内容覆盖 WASC

				分类的多种 Web 应用漏洞和 OWASP TOP10 网站漏洞进行管理；定期跟踪漏洞的修复情况从而使网站的漏洞得以快速修复，降低网站被入侵的风险。 5.利用 POC 对目标网页进行 WEB 漏扫，发现 SQL 注入漏洞、命令注入、CRLF 注入、LDAP 注入、XSS 跨站脚本漏洞、路径遍历漏洞、URL 跳转漏洞、文件包含漏洞、应用程序漏洞、文件上传漏洞、等安全漏洞问题。 6.使用模拟浏览器，爬虫 UA 等多种技术发现网站黑链，支持图片暗链的检测，支持全站对于潜藏在页面深处的第三方黄赌毒广告类链接进行监测并告警，可定位源代码黑链的位置和内容。支持配置监测频率，支持任务并发量配置，支持用户自定义黑词。 7.结合海量词库及人工识别，通过机器学习手段，提供敏感词发现的技术手段，支持全站监测，可定位敏感词位置和内容。涉及敏感词样本 5000+。支持配置监测频率，支持任务并发量配置，支持用户自定义敏感词，支持网页附件内容检测。 8.WEB 服务可用性监测，支持华北、华东、华南、海外机房 20 个检测节点，确保电信、联通和移动都具备监测点；支持网站故障原因定位，不限于：响应连接被重置、连接超时、http 状态码、连接被拒绝等。 9.支持 get/head/post 三种方式对 HTTP/HTTPS 服务进行监控，监控频率支持自定义。支持添加域名时识别 IP 协议栈情况，并且根据识别结果分别配置 IPv4 和 IPv6 的监测节点。 10.支持华北、华东、华南、海外机房≥20 个 DNS 监测节点，确保电信、联通和移动都具备监测点；支持 A 记录更改监测，网站 A 记录解析更变时可进行告警，告警支持短信/邮件方式。 11.支持展示网站目录结构，以树形模式展示。支持列表展示网站存在的外链及坏链，并提供指定连接检索能力。 12.支持对录入资产进行 IPv4/IPv6 检测，并根据检测结果对资产进行可用性监测，持根据添加资产的域名/ip 发现未知资产。 13.能够查看被通知的基本信息、安全告警列表。提供通知处理过程的时间轴，并可追踪通知处理的全过程，可对相关人的处理行为进行记录。 14.★支持日报、周报、月报、季报的生成；支持自定义周期性报告内容，包括自定义报告覆盖的资产、告警类型等（**投标**

				文件需提供能够体现上述功能配置选项截图复印件）。 15.支持多级账号管理，同级账号多角色管理，包含管理员、运维人员、普通运维人员；支持母账号对子账号登录的一键切换；支持子账号的密码修改、账号新建。 16.提供云端 7x24 小时告警人工运营服务，并提供问题处置建议和咨询；具有重大活动运营支撑服务。
22	安全服务	项	1	**一、定期安全评估服务** 为满足等级保护 2.0 关于定期全面网络安全检查、漏洞和安全风险评估的要求，3 年项目期内每年对医院整体信息系统开展 1 次全面的网络安全技术性评估工作，从如下方面开展评估： **（一）网络架构分析：**参照网络安全等级保护 2.0 的要求，从网络基础架构全局角度，评估桂林医学院附属医院业务系统在网络层面的防护情况，以发现医院现阶段网络架构防护的不足及风险，以为持续改进和提升医院安全防护提供方向和指导。 **（二）基础环境评估：**对桂林医学院附属医院重要业务系统（如 pas、His）等相关的服务器、数据库、中间件等，开展全面的基础环境评估工作，以评估检测业务系统基础环境（网络安全设备、服务器、数据库、中间件等）资产在漏洞补丁、安全配置方面的漏洞，识别可能存在的技术安全风险，基础环境评估包括安全漏洞扫描、安全基线配置核查两部分内容。 **1.安全漏洞扫描：**利用自动化漏洞扫描工具对核心关键设备如服务器、数据库、中间件等，使用带有安全漏洞知识库的网络安全扫描工具对有关资产进行安全脆弱性扫描，对被评估目标进行覆盖面广泛的安全漏洞查找，全面地反映主机系统、数据库系统以及中间件设备所存在的网络安全问题和面临的网络安全威胁，完成扫描后输出《安全漏洞扫描报告》。 安全服务商需自行提供安全漏洞扫描所需的脆弱性自动化检测工具，工具应具备对 DNS 服务的安全漏洞检查，包括 DNS 缓存中毒、DNS 拒绝服务漏洞、签名欺骗等至少 100 种以上的相关漏洞库；具备对 iOS、Android、Blackberry、windowsphone 等操作系统，并提供至少 50 种以上的相关漏洞库；具备对后门检测的安全漏洞检查，包括对 Microsoft IIS 特洛伊木马检测、Mac OS X 恶意程序等常见后门漏洞的安全检测，并提供至少 100 种以上的相关漏洞库。 **2.安全基线配置核查：**对医院核心关键设备如服务器、数据

				库、中间件等开展安全基线检查服务，通过“自动化工具配合人工检查”方式对关键设备的安全配置进行检查，以检测和发现关键设备在安全配置商存在的安全问题和不足，识别安全配置层面存在的安全风险。完成核查后输出《安全配置检查报告》 **（三）蓝队（攻击队）评估** 以实战化的视角，采用最大限度模拟 APT 攻击手法，以不采用破坏性攻击为底线，以系统提权、控制业务、获取数据为目标，对桂林医学院附属医院选定靶标系统可能存在的网络安全攻击路径和风险进行深度评估，以有效发现当前防御体系存在的问题和不足，评估医院整体安全防护体应对实战化攻击的有效性。攻击完成后输出《蓝队（攻击队）评估报告》。 **（四）互联网资产暴露面评估** 针对桂林医学院附属医院互联网暴露的域名/IP 进行梳理，全面检测发现互联网出口对外开放的已知和未知互联网资产，形成包括域名、IP、服务端口、应用服务等在内的互联网暴露资产信息，识别出非正常使用资产、无用僵尸资产、高危风险资产等关键资产信息，协助医院掌握外部资产风险，探测完成后出具《互联网资产暴露面评估报告》，并提供相应的安全建议。 3 年项目期内每年提供 1 次定期安全评估服务，评估完成后根据上述评估内容和结果，整理、汇总总体安全风险情况，输出整体的《安全评估报告》。 **二、实战攻防演习防守服务** 为有效应对自治区实战攻防演练活动，降低被攻击队攻破风险，提高医院实战攻防防护能力，3 年项目期间内每年为医院提供 1 次实战攻防演习防守服务，服务内容包括高危风险检测排查、攻防演习监测值守两部分服务内容，具体工作要求如下： **（一）高危风险检测排查** **1.互联网高危资产排查：**每年在自治区攻防演习活动开始前开展 1 次互联网高危资产排查工作，对桂林医学院附属医院的互联网高风险资产进行专项检测排查，通过网络空间资产探测技术，发现桂林医学院附属医院暴露在互联网上诸如远程运维端口、数据库端口、测试系统等高危风险问题，避免被攻击队攻击利用，完成检测后出具《互联网高危风险资产检测报告》。 **2.互联网侧重点系统渗透测试：**每年在自治区攻防演习活动开始前开展 1 次互联网侧重点系统渗透测试工作，在医院的授权

				和监督下，利用安全服务商已掌握的漏洞信息和攻击方式，针对互联网侧指定的 15 个业务系统开展非破坏性的模拟黑客攻击测试，以发现可能被攻击队利用的技术风险和弱点，并指导、协助用户对漏洞进行修复，以增强互联网测的安全能力。 安全服务在开展渗透测试中应充分结合使用渗透测试专家经验和自动化渗透测试工具，通过自动化渗透测试工具提高渗透测试的效率。自动化渗透测试具有“计算机软件著作权”，要求能够实可实现自动化渗透测试，贯穿整个渗透过程的操作，包括信息收集、漏洞探测、权限维持、报告生成等；可以根据可编程平台提供的接口编写自己的攻击插件，实现自定义的攻击需求；可利用 http 协议、DNS 协议等远程获取带外数据；可通过内置的方法反弹交互 shell 到平台，执行 vim、交互执行操作等功能。 **（二）攻防演习监测值守** 每年在自治区实战攻防演练期间提供 1 名攻防安全人员开展为期 7 天的 5*12 监测值守服务（8:00-21:00），现场开展如下监测值守服务工作： **1.威胁监控分析服务：**在自治区攻防演习期间，依托医院已有的全流量安全威胁监测设备，在攻防演习期间对攻击行为和安全事件进行实时、动态的监测，一旦发现有可疑攻击，立即按照攻防演习期间的上报流程，上报攻击事件，并协助医院技术人员及时对攻击事件进行处置。 **2.威胁专家研判服务：**在自治区攻防演习期间，依托医院已有的全流量安全威胁监测设备，提供威胁专家研判服务，协助进行复杂、深入的安全威胁和事件研判，并且对攻击影响范围、后果进行分析，发现安全防御体系和策略的实战缺陷，并配合进行紧急整改。 **3.应急响应服务：**在自治区攻防演习期间，提供突发网络安全事件应急响应处置和溯源分析服务，协助桂林医学院附属医院分析攻击来源、分析事件原因，编制《应急响应报告》等，并提出对应的安全建议。 在攻防演练的监测值守期间，现场服务人员将根据监测、研判、响应等情况编制相关监测分析、应急溯源、事件处置等报告，并按要求提交演练平台争取加分。 **4.攻防演习复盘总结服务：**在自治区攻防演习结束后，协助桂林医学院附属医院对自治区攻防演习的整个过程进行复盘分

				析，总结目前的优势和存在的问题。针对存在的问题，制定有针对性、可落地的改进建议并协助整改。 **三、驻场安全运营服务** 3 年项目服务期提供 1 名安全运营服务驻场人员，根据医院要求作息，负责医院日常的安全运营服务实施，并根据医院的需求提供专业服务支撑，驻场安全运营服务包括如下内容： **（一）定期安全漏洞扫描** 依据《信息安全技术 网络安全等级保护基本要求 》（GBT22239-2019）关于漏洞和风险管理的安全要求，为做好安全漏洞识别和管理工作；要求安全运营驻场服务人员每 2 个月开展 1 次安全漏洞扫描工作，对核心关键设备如服务器、数据库、中间件等，使用带有安全漏洞知识库的网络安全扫描工具对有关资产进行安全脆弱性扫描，对被评估目标进行覆盖面广泛的安全漏洞查找，全面地反映主机系统、数据库系统以及中间件设备所存在的网络安全问题和面临的网络安全威胁，在安全脆弱性扫描工作实施结束后，出具对应的《安全脆弱性报告》，其中包括安全脆弱性原理及相关修复建议，并提供相应的技术支持协助修复漏洞。 3 年项目服务期内每 2 个月开展 1 次，共 18 次。 **（二）定期安全配置核查** 参照《信息安全技术网络安全等级保护基本要求》（GBT22239-2019）关于计算环境安全的要求，要求安全运营驻场服务人员每半年开展 1 次安全配置核查工作，通过“自动化工具配合人工检查”方式参考安全配置基线进行检查，检查对象包括网络设备、安全设备、操作系统、数据库、中间件等安全配置基线，采用主流的安全配置核查系统或检查脚本工具完成安全基线配置的核查，核查工作完成后出具对应的《安全基线核查报告》，其中包括基线检查不合规项及相关修复建议，并提供相应的技术支持协助修复配置。 3 年项目服务期内每半年开展 1 次，共 6 次。 **（三）常态化安全监测分析** 依据《信息安全技术 网络安全等级保护基本要求 》（GBT22239-2019）关于“应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行为的攻击”安全监测分析要求，项目服务期间由安全运营驻场服务人员依托桂林医学院附

				属医院内部全流量高级威胁监测设备并结合其他安全设备的告警信息，为医院提供 5X8（每周 5 天，每天 8 小时）的实时安全监控服务，及时监测发现网络攻击行为和威胁，监测内容包括但不限于网络攻击、WEBSHELL 上传、弱口令、挖矿病毒等网络威胁，实时监测和发现信息网络基础设施的安全攻击及安全异常事件，发现攻网络攻击等异常事件时及时进行预警警示，并协助开展攻击事件处置。要求定期输出《安全监测分析报告》。 3 年项目服务期开展常态化监测分析，每月定期输出《安全监测分析报告》。 **（四）重要时期安全监测值守** 在两会、东盟博览会等重大敏感时期提供网络安全值守监测服务，对各类威胁和事件进行实时监测，对可能出现的网络安全事件提供应急响应支持，协助安全事件处置，工作要求如下： 1.重要时期安全保障期间，由安全运营驻场服务人员提供现场值守服务，重点依托各类安全设备开展威胁监测分析、攻击行为检测响应等工作，每日出具安全保障监测日报。 2.针对可能出现的网络安全事件，提供二线专家应急响应服务，协助快速处置安全事件，要求发生安全事件时 15 分钟内电话响应，4 小时内二线专家到达现场协助安全事件处置响应。 特殊时期安全保障时间主要包括全国两会（7 天）、自治区两会（5 天）、 中国-东盟“两会”（至少 5 天）等重点时间。安全保障期间每日输出《安全保障工作日报》，保障完成后输出《安全保障总结报告》。 **（五）网络安全迎检工作协助** 在网络安全监管单位或上级监管单位在医院执行网络安全监管检查时，协助医院安全管理人员开展网络安全迎检准备、配合现场安全检查等工作。 **（六）网络安全管理工作协助** 根据医院的工作需求，协助医院安全管理人员开展其他日常网络安全管理工作。
23	等级保护测评服务	项	1	一、总的要求 依照《信息安全技术--信息系统安全等级保护基本要求》（GB/T 22239-2019）、《信息系统安全等级保护测评准则》要求，对桂林医学院附属医院 2 个信息系统进行等级保护测评，指导采购人制定整改方案和开展整改，逐一出具符合国家信息安全

				等级保护管理部门规范要求、公安机关认可的信息系统安全等级测评报告。 二、依据标准 1.《计算机信息系统安全保护等级划分准则》（GB 17859-1999) 2.《信息安全等级保护管理办法》（公通字[2007]43 号） 3.《网络安全等级保护定级指南》（GB/22240-2020） 4.《网络安全等级保护基本要求》（GB/T 22239-2019） 5.《网络安全等级保护测评要求》（GB/T 28448-2019） 6.《网络安全等级保护测评过程指南》（GB/T 28449-2018) 7.《网络安全等级保护设计技术要求》（GB/T 25070-2019） 8.《网络安全等级保护测试评估技术指南》（GB/T 36627-2018） 三、测评内容： （1）安全通用要求 安全通用要求测评内容应包括安全技术和安全管理两大类，其中技术类应包括对安全物理环境、安全通信网络、安全区域边界、安全计算环境、安全管理中心五个方面的测评，安全管理类测评应包括对安全管理制度、安全管理机构、安全管理人员、安全建设管理、安全运维管理五个方面的测评。 （2）安全扩展要求 应用不同新技术的安全保护对象处于不同的应用场景中，面临不同的安全威胁，会有不同的安全需求，该保护对象涉及的安全扩展要求包括： 1）云计算 云计算安全测评内容包括对安全物理环境、安全通信网络、安全区域边界、安全计算环境、安全管理中心、安全建设管理、安全运维管理等的测评。 2）移动互联 移动互联安全测评内容包括对安全物理环境、安全区域边界、安全计算环境、安全建设管理、安全运维管理等的测评。 3）物联网 物联网安全测评内容包括对安全物理环境、安全区域边界、安全计算环境、安全运维管理等的测评。 4）工业控制系统

				工业控制系统安全测评包括对安全物理环境、安全通信网络、安全区域边界、安全计算环境、安全建设管理方面的测评。 5)大数据 大数据安全测评包括对安全物理环境、安全通信网络、安全计算环境、安全运维管理等的测评。 四、测评方法 在测评实施过程中，应采用访谈、检查和测试、渗透测试等测评方法进行，并与国家相关规范及标准的要求相符。 访谈是指测评人员通过引导信息系统相关人员进行有目的的（有针对性的）交流以帮助测评人员理解、分析或取得证据的过程； 检查是指测评人员通过对测评对象（如管理制度、操作记录、安全配置等）进行观察、查验、分析以帮助测评人员理解、分析或取得证据的过程； 测试是测评人员使用预定的方法/工具使测评对象产生特定的行为，通过查看和分析结果以帮助测评人员获取证据的过程； 渗透测试是模拟黑客的攻击方法，对受保护对象的应用系统、主机、网络进行攻击，从而验证测评对象的弱点、技术缺陷或漏洞的一种评估方法； 渗透测试是模拟黑客的攻击方法，对受保护对象的应用系统、主机、网络进行攻击，从而验证测评对象的弱点、技术缺陷或漏洞的一种评估方法。 五、服务成果 测评完成后，出具一式三份符合等保2.0相关技术标准要求、国家网络安全等级保护管理部门规范要求且公安机关认可的网络安全等级保护测评报告。

三、商务要求

1. 报价要求

本次报价须为人民币报价，包含服务交付成果、设计、组织、策划、开发、调研、技术协助、校准、培训、技术指导、产品价、运输费（含装卸费）、保险费、安装调试费、税费、产品检测费、产品质保期内维护费等类似服务内容的全部费用。对于本文件中明确列明必须报价的货物或服务，供应商应分别报价。对于本文件中未列明，而供应商认为必需的费用也需列入总报价。在合同实施时，采购人将不予支付中标供应商没有列入的项目费用，并认为此项目的费用已包括在投标总报价中。

2.合同签订日期

中标通知书发出后 25 日内。

3.交货（实施）时间

自签订合同之日起 180 个日历日内完成网络安全建设

4.交货地点或服务地点

广西桂林市内采购人指定地点。

5.验收标准

详见招标文件合同主要条款格式部分

6.服务标准、期限、效率

6.1 中标供应商在质量保证期内应当为采购人提供以下技术支持和服务：

6.1.1 电话咨询

中标供应商应当为采购人提供技术援助电话，解答采购人在使用中遇到的问题，及时为采购人提出解决问题的建议。

6.1.2 现场响应

采购人遇到使用或技术问题，电话咨询不能解决的，中标供应商应在 6 小时内到达现场进行处理，到达现场后 2 小时内排除故障，恢复正常使用。

6.1.3 技术升级

在质保期内，如果中标供应商的产品或服务升级，中标供应商应及时通知采购人，如采购人有相应要求，中标供应商应对采购人购买的产品或服务进行升级。

7.培训

供应商对其提供产品或服务的使用和操作应尽培训义务。供应商应提供对采购人的基本培训，使采购人使用人员熟练掌握所培训内容，熟练掌握全部功能，培训的相关费用包括在投标报价中，采购人不再另行支付。

8.付款方式、时间及条件

合同签订后 5 个工作日内支付合同总额 30%的预付款；按照等保三级要求部署，并且顺利通过三级等保测评，支付合同总金额 30%的项目款；全部部署完成，调试无误，设备整体验收，顺利通过攻防演练（不被攻破），经采购人验收合格并签发验收合格单后支付总金额 20%；下一年顺利通过攻防演练（不被攻破），支付余下合同总额 20% (无息)。采购人付款前，中标供应商应向采购人开具符合采购人要求

的正规财务票据，否则采购人有权暂缓或拒付款项且不构成违约。

9.履约保证金

无

10.包装和运输要求

根据《财政部等三部门联合印发商品包装和快递包装政府采购需求标准（试行）》财办库【2020】123号文规定，若投标产品使用塑料、纸质、木质等包装材料时应满足《商品包装政府采购需求标准（试行）》要求，若投标产品需要快递包装，快递封装材料应满足《快递包装政府采购需求标准（试行）》要求。运输要求详见招标文件合同主要条款格式部分

11.售后服务

11.1 中标供应商应按照国家有关法律法规和“三包”规定以及招标文件、投标文件、合同及附件的规定，为采购人提供售后服务。中标供应商承诺质量保证期优于国家“三包”规定的，或优于招标文件规定的，按中标供应商实际承诺执行。

11.2 中标供应商应明确承诺招标文件采购需求部分如无特别要求，则质保期为自验收之日起 3 年，招标文件采购需求部分有特别要求的则以技术参数要求表为准。

11.3 质保期过后的服务要求

电话咨询：产品质量保证期过后，中标供应商应当为采购人提供技术援助电话，解答采购人在使用中遇到的问题，及时为采购人提出解决问题的建议，并不予收费。

12.保险

供应商负责办理运输和保险，将货物运抵交货地点。与运输、保险相关的费用由供应商承担。

四、其他要求

1、采购人有权要求中标供应商提供至少三年的驻场服务，供应商须在投标文件中提供承诺函，格式自拟。

2、“政采云平台”在线功能演示要求

（1）本项目招标文件第四章评审方法及标准“系统功能及联动能力分”，供应商可提供“政采云平台”在线功能演示予以佐证。供应商提供的在线功能演示可以以搭建的系统平台方式进行在线操作演示，也可以采用平台演示视频录像文件方式进行在线演示。

（2）供应商于投标截止时间当天上午 9 时 30 分后在规定时间内**按第四章评审方法及标准“系统功能及联动能力分”**要求通过“政采云”平台进行在线功能演示（具体演示时间以本项目评标委员会通知为准，供应商自行准备演示相关设备及网络等演示工具）

（3）供应商参与在线演示人员不得超过 1 人，演示时间应控制在 20 分钟以内。

（4）未参与演示或演示不符合要求得 0 分。

附件 1：

中小微企业划型标准

行业名称	指标名称	计量单位	中型	小型	微型
农、林、牧、渔	营业收入（Y）	万元	500≤Y＜20000	50≤Y＜500	Y＜50
工业	从业人员（X）	人	300≤X＜1000	20≤X＜300	X＜20
	营业收入（Y）	万元	2000≤Y＜40000	300≤Y＜2000	Y＜300
建筑业	营业收入（Y）	万元	6000≤Y＜80000	300≤Y＜6000	Y＜300
	资产总额（Z）	万元	5000≤Z＜80000	300≤Z＜5000	Z＜300
批发业	从业人员（X）	人	20≤X＜200	5≤X＜20	X＜5
	营业收入（Y）	万元	5000≤Y＜40000	1000≤Y＜5000	Y＜1000
零售业	从业人员（X）	人	50≤X＜300	10≤X＜50	X＜10
	营业收入（Y）	万元	500≤Y＜20000	100≤Y＜500	Y＜100
交通运输业	从业人员（X）	人	300≤X＜1000	20≤X＜300	X＜20
	营业收入（Y）	万元	3000≤Y＜30000	200≤Y＜3000	Y＜200
仓储业	从业人员（X）	人	100≤X＜200	20≤X＜100	X＜20
	营业收入（Y）	万元	1000≤Y＜30000	100≤Y＜1000	Y＜100
邮政业	从业人员（X）	人	300≤X＜1000	20≤X＜300	X＜20
	营业收入（Y）	万元	2000≤Y＜30000	100≤Y＜2000	Y＜100
住宿业	从业人员（X）	人	100≤X＜300	10≤X＜100	X＜10
	营业收入（Y）	万元	2000≤Y＜10000	100≤Y＜2000	Y＜100
餐饮业	从业人员（X）	人	100≤X＜300	10≤X＜100	X＜10
	营业收入（Y）	万元	2000≤Y＜10000	100≤Y＜2000	Y＜100
信息传输业	从业人员（X）	人	100≤X＜2000	10≤X＜100	X＜10
	营业收入（Y）	万元	1000≤Y＜100000	100≤Y＜1000	Y＜100
软件和信息技术服务业	从业人员（X）	人	100≤X＜300	10≤X＜100	X＜10
	营业收入（Y）	万元	1000≤Y＜10000	50≤Y＜1000	Y＜50
房地产开发经营	营业收入（Y）	万元	1000≤Y＜200000	100≤X＜1000	X＜100
	资产总额（Z）	万元	5000≤Z＜10000	2000≤Y＜5000	Y＜2000
物业管理	从业人员（X）	人	300≤X＜1000	100≤X＜300	X＜100
	营业收入（Y）	万元	1000≤Y＜5000	500≤Y＜1000	Y＜500
租赁和商务服务业	从业人员（X）	人	100≤X＜300	10≤X＜100	X＜10
	资产总额（Z）	万元	8000≤Z＜120000	100≤Z＜8000	Y＜100
其他未列明行业	从业人员（X）	人	100≤X＜300	10≤X＜100	X＜10

说明：上述标准参照《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），大型、中型和小型企业须同时满足所列指标的下限，否则下划一档；微型企业只须满足所列指标中的一项即可。

附件 2：

附

金融业企业划型标准

行业		类别	类型	资产总额
货币金融服务	货币银行服务	银行业存款类金融机构	中型	5000 亿元（含）至 40000 亿元
			小型	50 亿元（含）至 5000 亿元
			微型	50 亿元以下
	非货币银行服务	银行业非存款类金融机构	中型	200 亿元（含）至 1000 亿元
			小型	50 亿元（含）至 200 亿元
			微型	50 亿元以下
		贷款公司、小额贷款公司及典当行	中型	200 亿元（含）至 1000 亿元
			小型	50 亿元（含）至 200 亿元
			微型	50 亿元以下
资本市场服务		证券业金融机构	中型	100 亿元（含）至 1000 亿元
			小型	10 亿元（含）至 100 亿元
			微型	10 亿元以下
保险业		保险业金融机构	中型	400 亿元（含）至 5000 亿元
			小型	20 亿元（含）至 400 亿元
			微型	20 亿元以下
其他金融业	金融信托与管理服务	信托公司	中型	400 亿元（含）至 1000 亿元
			小型	20 亿元（含）至 400 亿元
			微型	20 亿元以下
	控股公司服务	金融控股公司	中型	5000 亿元（含）至 40000 亿元
			小型	50 亿元（含）至 5000 亿元
			微型	50 亿元以下
	其他未包括的金融业	除贷款公司、小额贷款公司、典当行以外的其他金融机构	中型	200 亿元（含）至 1000 亿元
			小型	50 亿元（含）至 200 亿元
			微型	50 亿元以下

第三章　供应商须知

供应商须知前附表

条款号	要点	内容、要求
1.3.1	项目基本信息	项目名称：桂林医学院附属医院一院两区网络安全建设项目 项目编号：GXZC2023-G3-003411-JDZB 采购计划号：广西政采[2023]16502 号
1.3.2	采购方式	公开招标。
1.4	促进中小企业发展措施	本项目为非专门面向中小微企业采购。
1.5.1	供应商资格条件	详见招标公告。
1.5.3	联合体	是否接受联合体详见招标公告
1.6	踏勘	否
1.7.2	分包	是否接受分包详见招标公告
2.3	招标文件澄清、修改	在招标公告发布媒介发布。
2.3	确认收到澄清、修改发布的方式	澄清、修改文件自招标公告发布媒体发布之日起，视为供应商已收到该澄清、修改。供应商未及时关注招标公告发布媒体造成的损失，由供应商自行负责。
3.4.1	投标有效期	投标截止之日起 90 天。
3.5	投标保证金	本项目无投标保证金
3.6	投标文件的编制	投标文件应按第六章投标文件格式分别编制并使用下载的政采云投标客户端制作并上传。
3.7	投标文件递交截止时间及开标时间	见招标公告要求。
4.2	备份投标文件	本项目 接受 备份投标文件 以政采云系统自动生成的备份文件为依据，当项目允许接受备份响应文件时，供应商才可以按规定上传备份响应文件。提交电子备份投标文件方式：**在接到无法解密或解密失败的通知后，供应商可根据自身实际情况按通知时要求的时间到桂林市公共资源交易中心_____号开标室现场提交或以电子邮件的形式（以通知时所告知的电子邮箱地址为准）提交电子备份投标文件**。供应商可以由法定代表人、负责人、自然人或其委托代理人出席开标会议。
4.3	演示	否
4.4	样品	否
6.5.1	结果公告	采购代理机构在采购人依法确认中标人后 2 个工作日内在招标公告发布的媒体上发布结果公告。
6.5.2	中标通知书	采购代理机构通过政采云平台发出中标通知书。 中标通知书在政采云平台推送之日起，视为中标人已收到，中标人自行承担

		未及时查收的后果。
6.5.3	招标结果通知书	采购代理机构通过电子邮件或书面方式发出招标结果通知书，供应商自行承担未及时查收的后果。
8.1	质疑	（1）供应商认为招标文件、采购过程、中标或者成交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 7 个工作日内，通过以下方式向采购人、采购代理机构提出质疑。提出质疑的供应商必须是参与本项目采购活动的供应商，并须在法定质疑期内一次性提出针对同一采购程序环节的质疑。质疑函应使用财政部发布的政府采购供应商质疑函范本，并应按照“质疑函制作说明”进行制作。 （2）本项目不接受传真、移动通信、政采云平台等方式送达的质疑材料，供应商可通过现场或邮寄方式递交书面质疑材料。供应商应于质疑有效期内将质疑函原件递交或邮寄至招标公告中采购代理机构信息中的联系人。
9.1	代理服务费	（1）代理服务费 ☑采购代理机构向中标供应商收取代理服务费。本项目代理服务费按照《招标代理服务费管理暂行办法》 (计价格〔2002〕1980 号)、《国家发展改革委关于降低部分建设项目收费标准规范收费行为等有关问题的通知》(发改价格〔2011〕534 号)规定的 70%采用差额定率累进法计算。具体费率如下： ①招标金额在 100 万元以下的： 货物 1.5%；服务招标 1.5%；工程招标 1.0%； ②招标金额在 100-500 万元之间： 货物 1.1%；服务招标 0.8%；工程招标 0.7%； ③招标金额在 500-1000 万元之间： 货物 0.8%；服务招标 0.45%；工程招标 0.55%； ④招标金额在 1000-5000 万元之间： 货物 0.5%；服务招标 0.25%；工程招标 0.35%； …… 差额定率累进法计算过程示例： 例如：某货物招标代理业务成交金额为 300 万元，招标代理服务费金额按如下计算： 100 万元×1.5%＝1.5 万元 （300－100）万元×1.1%＝2.2 万元 合计收费＝（1.5＋2.2）*70%=2.59 万元 （2）中标供应商在中标通知书发出前以银行转账或现金形式支付代理服务费。 开户银行：广西北部湾银行南宁市金湖支行 （银行地址：南宁市金湖路 57 号文德大厦 1 楼） 开户名称：广西机电设备招标有限公司 银行账号：1705012090027723 (联行号 313611017053) 财务联系人：吴茜（电话：0771-2821398）
9.3	附件	☑无
9.3	图纸	☑无
9.4	其他事项	本文件中内容如有前后不一致，以在招标文件先出现的为准。

1．总则

1.1 适用范围

本招标文件适用于供应商须知前附表所述项目的政府采购活动。

1.2 定义

1.2.1“采购人”系指依法进行政府采购的国家机关、事业单位、团体组织。

1.2.2“供应商”系指响应招标、参加投标竞争的法人、其他组织或者自然人。

1.2.3 本文件中的“法定代表人”若无特别说明，当供应商是企业的，是指企业法人营业执照上的法定代表人；当供应商是事业单位的，是指事业单位法人证书上的法定代表人；当供应商是社会团体、民办非企业的，是指法人登记证书中的法定代表人；当供应商是个体工商户的，是指个体工商户营业执照上的经营者；当供应商是自然人的，是指参与本项目响应的自然人本人。

1.2.4 本文件中的“公章”是指根据我国对公章的管理规定，用供应商法定主体行为名称制作的印章，除本文件有特殊规定外，供应商的财务章、部门章、分公司章、工会章、合同章、投标专用章、业务专用章及银行的转账章、现金收讫章、现金付讫章等其他形式印章均不能代替公章。本文件中的“签章”是指电子签名的一种表现形式，利用图像处理技术将电子签名操作转化为与纸质文件盖章操作相同的可视效果，同时利用电子签名技术保障电子信息的真实性和完整性以及签名人的不可否认性。

1.2.5“书面形式”如无特殊规定，书面形式是合同书、信件、电报、电传等可以有形地表现所载内容的形式。以电子数据交换、电子邮件等方式能够有形地表现所载内容，并可以随时调取查用的数据电文，视为书面形式。招标文件如有特殊规定，以招标文件规定为准。

1.2.6 本项目的技术商务要求重要性分为“▲”（如有）、“★”（如有）和一般无标识指标。▲代表实质性要求指标，**不满足该指标项将导致投标被否决**，★代表重要指标，无标识则表示一般指标项。

1.2.7 本招标文件出现多种选项的条款，以“☑”表示本条款所选择的方式。

1.2.8 “电子交易平台”是指以数据电文形式在线完成采购活动的信息平台，本招标文件中也称“政采云平台”。

1.3 项目信息

1.3.1 项目名称及编号：详见供应商须知前附表

1.3.2 采购方式：详见供应商须知前附表

1.4 促进中小企业发展政策

1.4.1 本项目落实促进中小企业发展政策措施在前附表规定。依据促进中小企业发展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。

根据《政府采购促进中小企业发展管理办法》（财库[2020]46 号）第九条、《广西壮族自治区财政厅关于进一步发挥政府采购政策功能促进企业发展的通知》（桂财采[2022]30 号）、以及《广西壮族自治区财政厅 广西壮族自治区工业和信息化厅转发财政部 工业和信息化部政府采购促进中小企业发展管理办法的通知》（桂财采[2021]70 号）规定，价格扣除比例在第四章评审方法及标准中规定，对小型企业和微型企业同等对待，不作区分。

1.4.2 中小企业定义

1.4.2.1 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。

1.4.2.2 供应商提供的货物、工程或者服务符合下列情形的，享受本款规定的促进中小企业发展政策：

在货物采购项目中，货物由中小企业制造，即货物由中小企业生产且使用该中小企业商号或者注册商标；

在工程采购项目中，工程由中小企业承建，即工程施工单位为中小企业；

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。

在货物采购项目中，供应商提供的货物既有中小企业制造货物，也有大型企业制造货物的，不享受本款规定的促进中小企业发展政策。

1.4.2.3 本项目标的所属行业在第二章采购需求中规定。供应商根据中小企业划分标准（《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）判断是否为中小企业。（见附件）

符合条件的货物制造商、工程施工单位、服务承接单位为中小企业的，应按招标文件规定在投标文件中提供声明函。

1.4.2.4 视同中小企业情形

（1）符合中小企业划分标准的个体工商户，视同中小企业。

（2）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）符合《财政部、司法部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，或符合《关于促进残疾人就业政府采购政策的通知》（财库〔2017〕141 号）规定的残疾人福利性单位，视同小型、微型企业。

符合条件的货物制造商、工程施工单位、服务承接单位为监狱企业或残疾人福利性单位的，应按招标文件规定在投标文件中提供相关证明文件。

1.5 供应商资格要求

1.5.1 供应商资格要求：详见供应商须知前附表

1.5.2 按照招标公告的规定获得招标文件。

1.5.3 本项目是否接受联合体投标，见“供应商须知前附表”规定。

如接受联合体投标，联合体投标要求如下：

（1）供应商可以组成一个投标联合体，以一个供应商的身份共同参加投标。联合体投标的，须提供《联合体协议书》（格式后附）

（2）以联合体形式参加投标的，联合体各方均必须具备《中华人民共和国政府采购法》第二十二条第一款规定的基本条件。本项目有特殊要求规定供应商特定条件的，联合体各方中至少有一方必须符合招标文件规定的特定条件。

（3）联合体各方之间必须签订联合体协议，协议书必须明确主体方（或者牵头方）并明确约定联合体各方承担的工作和相应的责任，并将联合投标协议放入投标文件。联合体各方必须共同与采购人签订采购合同，就采购合同约定的事项对采购人承担连带责任。

（4）以联合体形式参加政府采购活动的，联合体各方不得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。

（5）联合体中有同类资质的供应商按照联合体分工承担相同工作的，应当按照资质等级较低的供应商确定资质等级。

（6）联合体投标业绩、履约能力按照联合体各方其中较高的一方认定并计算（招标文件其他章节另有规定的除外）。

（7）供应商为联合体的，可以由联合体中的一方或者多方共同交纳投标保证金，其交纳的保证金对联合体各方均具有约束力。

（8）联合体各方均应按照招标文件的规定提交资格证明文件。

1.6 现场踏勘及投标费用

1.6.1 前附表如规定现场踏勘的，供应商应按规定时间地点参加踏勘。

1.6.2 供应商均应自行承担所有与投标有关的全部费用（招标文件有相关的规定除外）。

1.7 转包与分包

1.7.1 如招标文件其他地方无特别规定，本项目不允许转包。

1.7.2 本项目是否允许分包详见“供应商须知前附表”，本项目不允许违法分包。供应商根据招标文件的规定和采购项目的实际情况，拟在中标后将中标项目的非主体、非关键性工作分包的，应当在投标文件中载明分包承担主体，分包承担主体应当具备相应资质条件且不得再次分包。

1.8 特别说明

1.8.1 供应商应保证其提供的联系方式（电话、传真、电子邮件）有效，以保证往来函件（澄清、修改等）能及时通知供应商，并能及时反馈，否则采购人及代理机构不承担由此引起的一切后果。

1.8.2 供应商应仔细阅读招标文件的所有内容，按照招标文件的要求提交投标文件，并对所提供的全部资料的真实性承担法律责任。

1.8.3 供应商在投标活动中提供任何虚假材料，将报监管部门查处；

2．招标文件

2.1 招标文件的构成

第一章 招标公告

第二章 采购需求

第三章 供应商须知

第四章 评审方法及标准

第五章 合同主要条款格式

第六章 投标文件格式

2.2 供应商的风险

供应商没有按照招标文件要求提供全部资料，或者供应商没有对招标文件在各方面作出实质性响应是供应商的风险，并可能导致其投标被否决。

2.3 招标文件的澄清与修改

2.3.1 任何已获得招标文件的潜在供应商，均可以书面形式要求采购代理机构作出书面解释、澄清。

2.3.2 采购人、采购代理机构对已发出的招标文件进行必要澄清或者修改的，采购人或者采购代理机构可以对已发出的招标文件进行必要的澄清或者修改。澄清或者修改的内容可能影响投标文件编制的，采购人或者采购代理机构应当在投标截止时间至少 15 日前，在供应商须知前附表规定的方式通知所有获取招标文件的潜在供应商；不足 15 日的，采购人或者采购代理机构应当顺延提交投标文件的截止时间。

2.3.3 招标文件澄清、答复、修改、补充的内容为招标文件的组成部分。当招标文件与招标文件的答复、澄清、修改、补充通知就同一内容的表述不一致时，以最后发出的公告或书面文件为准。

3．投标文件

3.1 投标文件的组成

投标文件由第六章“投标文件格式”规定的内容和供应商所作的一切有效补充、修改和承诺等文件组成。

3.2 投标文件的语言及计量

3.2.1 投标文件以及供应商与采购人就有关投标事宜的所有来往函电，均应以中文书写（除专用术语外，与招标投标有关的语言均使用中文。必要时专用术语应附有中文注释）。供应商提交的支持文件和印刷的文献可以使用别的语言，但其相应内容应同时附中文翻译文本，在解释投标文件时以中文翻译文本为主。对不同文字文本投标文件的解释发生异议的，以中文文本为准。

3.2.2 计量单位招标文件已有明确规定的，投标使用招标文件规定的计量单位；招标文件没有规定的，应采用中华人民共和国法定计量单位。

3.3 投标报价

3.3.1 投标报价应按招标文件中相关附表格式填写。

3.3.2 投标文件只允许有一个报价，有选择的或有条件的报价将不予接受。

3.3.3 对于本文件中未列明，而供应商认为必需的费用也需列入投标报价。在合同实施时，采购人将不予支付中标人没有列入的项目费用，并认为此项目的费用已包括在投标报价中。

3.3.4 采购人不接受供应商给予的赠品、回扣或者与采购无关的其他商品、服务。

3.4 投标有效期

3.4.1 如招标文件其他地方无特别规定，投标有效期则为投标截止之日起 90 天。在投标有效期内投标文件应保持有效。**有效期不足的投标文件将被否决**。

3.4.2 在特殊情况下，采购人可与供应商协商延长投标文件的有效期，这种要求和答复均以书面形式进行。

3.4.3 供应商同意延长的投标有效期的，如本项目要求提交保证金则应相应延长其投标保证金的有效期，但不得要求或被允许修改或撤销其投标文件；供应商拒绝延长的，其投标无效，但供应商有权收回其投标保证金。

3.5 投标保证金

3.5.1 供应商须按须知前附表规定提交投标保证金，**否则其投标将被否决**。除招标文件规定不予退还保证金的情形外，代理机构在规定时间内退回供应商的投标保证金（供应商自行承担因未按供应商须知前附表要求交纳导致投标保证金无法及时退还的责任）。

3.5.2 投标保证金币种应与投标报价币种相同。

3.5.3 未中标人的投标保证金在中标通知书发出后 4 个工作日内退还。中标人的投标保证金在合同签订后 4 个工作日内退还（办理退还手续时需要向采购代理机构提供两份合同复印件）。

3.5.4 供应商有下列情形之一的，投标保证金将不予退还：

（1） 供应商在投标有效期内撤销投标文件的；

（2） 供应商在投标过程中弄虚作假，提供虚假材料的；

（3） 中标人无正当理由不与采购人签订合同的；

（4） 将中标项目转让给他人或者在投标文件中未说明且未经采购人同意，将中标项目分包给他人的；

（5） 拒绝履行合同义务的；

（6） 其他严重扰乱招投标程序的。

3.6 投标文件的编制要求

3.6.1 供应商应先安装“政采云投标客户端”（请自行前往“政采云”平台进行下载），通过账号密码或 CA 登录客户端制作投标文件。

3.6.2 供应商应按本招标文件规定的格式和顺序编制投标文件并进行关联定位，以便评标委员会在评审时，点击评分项可直接定位到该评分项内容。如对招标文件的某项要求，供应商的投标文件未能关联定位提供相应的内容与其对应，则评标委员会在评审时如做出对供应商不利的评审由供应商自行承担。投标文件如内容不完整、编排混乱导致投标文件被误读、漏读，或者在按招标文件规定的部位查找不到相关内容的，由供应商自行承担。

3.6.3 供应商的投标文件未按照招标文件要求签署、盖章的，**其投标无效**。

3.6.4 为确保网上操作合法、有效和安全，供应商应当在投标截止时间前完成在“政采云”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。

3.6.5 投标文件中标注的供应商名称应与主体资格证明（如营业执照、事业单位法人证书、执业许可证、个体工商户营业执照、自然人身份证等）和公章/电子签章一致，**否则作无效投标处理。**

3.7 投标文件的递交、修改和撤回

3.7.1 供应商必须在“供应商须知前附表”规定的投标文件开标时间和投标地点提交电子版投标文件。电子投标文件应在制作完成后，在投标截止时间前通过有效数字证书（CA 认证锁）进行电子签章、加密，然后通过网络将加密的电子投标文件递交至“政采云平台”。

3.7.2 未在规定时间内提交或者未按照招标文件要求签章、加密的电子投标文件，“政采云”平台将拒收。

3.7.3 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，“政采云”平台将拒收。

3.7.4 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。

3.7.5 在投标截止时间止提交电子版投标文件的供应商不足 3 家时，电子版投标文件由代理机构在“政采云”平台操作退回，除此之外采购人和采购代理机构对已提交的投标文件概不退回。

3.7.6 招标文件未允许同一供应商提交两个或以上不同的响应文件，但存在同一供应商提交两个或以上不同的响应文件的，**其投标无效。**

4．开标

4.1 开标准备

本项目投标截止时间及地点见“供应商须知前附表”规定。

全流程电子化项目没有现场递交投标文件及现场开标环节。采购代理机构将按照招标文件规定的时间通过“政采云”平台组织线上开标活动、开启投标文件，所有供应商均应当准时在线参加。供应商如不参加开标大会的，视同认可开标结果，事后不得对采购相关人员、开标过程和开标结果提出异议，同时供应商因未在线参加开标而导致投标文件无法按时解密等一切后果由供应商自己承担。

如供应商成功解密投标文件，但未在“政采云”电子开标大厅参加开标的，视同认可开标过程和结果，由此产生的后果由供应商自行负责。

4.2 开标程序

4.2.1 供应商登录政采云平台进入开标大厅签到。

4.2.2 解密电子投标文件。“政采云”平台按开标时间自动提取所有投标文件。采购代理机构在“政采云”平台向各供应商发出电子加密投标文件开始解密通知，由供应商平台设置时间内自行进行投标文件解密。供应商须使用加密时所用的 CA 锁准时登录到“政采云”平台电子开标大厅签到并对电子投标文件解密。开标后供应商未及时进行解密的，代理机构可通知供应商。通知后供应商仍未在上述规定时间内解密响应文件，或者供应商没预留联系方式或预留联系方式无效导致代理机构无法联系到供应商进行解密的，均视为无效投标。

4.2.3“政采云”平台设置有备份响应文件功能。备份响应文件是指平台设置为接受备份响应文件时，如出现供应商上传的响应文件存在问题或其他供应商原因引起解密异常时，供应商可以在规定时间内将备份响应文件通过邮箱发送至采购代理机构，由代理机构上传备份响应文件后自动解密从而避免被视为无效响应。是否接受备份响应文件详见供应商须知前附表，如接受备份文件，供应商未在规定时间内发送备份响应文件的将视为无效响应。

4.2.4 解密异常情况处理：详见本章 9.2 电子交易活动的中止。

4.2.5 供应商对报价进行确认。

4.2.6 开标结束。

特别说明：如遇“政采云”平台电子化开标或评审程序调整的，按调整后的程序执行。

4.3 演示

4.3.1“供应商须知前附表”规定在开标会议结束后进行演示的，供应商应按规定进行演示。

4.3.2 未按规定时间进行演示可能引起的演示分数被计为 0 分或投标无效等后果由供应商自行承担。

4.4 样品

4.4.1“供应商须知前附表”规定递交样品的，供应商应按前附表规定递交样品，递交样品时应附样品递交表（格式见第六章）。

4.4.2 未按规定时间递交样品可能引起的样品分数被计为 0 分或投标无效等后果由供应商自行承担。

4.4.3 样品封存或退还的说明请见第六章投标文件格式所附样品递交表。

5．资格审查

5.1 开标结束后，采购人或者采购代理机构通过电子交易平台对供应商的资格进行审查。资格审查是根据法律法规和招标文件的规定，对供应商的基本资格条件、特定资格条件进行审查。

5.2 资格审查标准在第四章评审方法及标准中规定，符合资格审查标准要求的供应商即为资格审查合格。

5.3 供应商有下列情形之一的，资格审查不合格，作无效投标处理：

5.3.1 不具备招标文件中规定的资格要求或资格条件的；（注：其中信用查询规则见“供应商须知前附表”，“政采云”平台已与“信用中国”平台做接口，审查专家可直接在线查询）

5.3.2 投标文件缺少任何一项资格证明文件或不符合第四章评审方法及标准中资格审查标准规定的评审内容的；

5.4 资格审查合格的供应商不足 3 家的，不得评审。

6．评审

6.1 评标委员会及评审原则

6.1.1 本项目评审工作由评标委员会负责，评标委员会由评审专家和采购人代表（如有）组成。评标委员会评审时必须公平、公正、客观，不带任何倾向性和启发性；不得向外界透露任何与评审有关的内容；任何单位和个人不得干扰、影响评标的正常进行；评标委员会及有关工作人员不得私下与供应商接触，不得收受利害关系人的财物或者其他好处；评审专家发现本人与参加采购活动的供应商有利害关系的，应当主动提出回避。

6.1.2 评标委员会成员应当通过电子交易平台进行独立评审，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审报告上签署不同意见及理由，否则视为同意评审报告。如果在评审过程中出现法律法规和招标文件均没有明确规定的情形时，由评标委员会现场协商确定，协商不一致的，由全体评标委员会成员投票表决，应当按照少数服从多数的原则作出结论并由采购代理机构记录在评审报告中。

6.1.3 采购人、采购代理机构应当采取必要措施，保证评审在严格保密（封闭式评审）的情况下进行。除采购人代表、评审现场组织人员外，采购人的其他工作人员以及与评审工作无关的人员不得进入评审现场。有关人员对评审情况以及在评审过程中获悉的国家秘密、商业秘密负有保密责任。

6.1.4 本项目评审过程实行全程网上留痕及录音、录像监控，供应商在评审过程中所进行的试图影响评审结果的不公正活动，可能导致其投标按无效处理。

6.2 评审方法及依据

6.2.1 本项目采用第四章评审方法及标准规定的方法进行评审。

6.2.2 评标委员会以招标文件、补充文件、投标文件、澄清及答复为评审依据，第四章评审方法及

标准没有规定的评审方法、标准及因素，不得作为评审依据。

6.3 评审程序

6.3.1 符合性审查

资格审查结束后，评标委员会对通过资格审查的供应商的投标文件进行报价、商务资信、技术等方面实质性内容进行符合性审查，符合性审查标准详见第四章评审方法及标准。

6.3.2 强制性采购要求（仅适用于货物采购项目）

（1）根据《财政部 发展改革委 生态环境部 市场监管总局关于调整优化节能产品、环境标志产品政府采购执行机制的通知》（财库〔2019〕9 号）和《关于印发节能产品政府采购品目清单的通知》（财库〔2019〕19 号）规定，本项目采购需求中的产品属于节能产品政府采购品目清单内标注“★”的，供应商的投标货物必须使用政府强制采购的节能产品，否则投标文件作无效处理；属于品目清单内非标注“★”的产品时，应优先采购。

（2 ）根据《关于调整网络安全专用产品安全管理有关事项的公告》（2023 年 1 号）规定，本项目采购需求中的产品如果包括《网络关键设备和网络安全专用产品目录》的网络安全专用产品，供应商在投标文件中应主动列明供货范围中属于网络安全专用产品的投标产品，并提供由中共中央网络安全和信息化委员会办公室网站最新发布的《网络关键设备和网络安全专用产品安全认证和安全检测结果》截图证明材料，不在《网络关键设备和网络安全专用产品安全认证和安全检测结果》中或不在有效期内或未提供有效的《计算机信息系统安全专用产品销售许可证》的，投标无效。

注：网络安全专用产品在中共中央网络安全和信息化委员会办公室网站上发布的《网络关键设备和网络安全专用产品目录》中查询。 目前共 15 类：路由器、交换机、服务器（机架式）、可编程逻辑控制器（PLC 设备）、数据备份一体机、防火墙（硬件）、WEB 应用防火墙（WAF）、入侵检测系统（IDS）、入侵防御系统（IPS）、安全隔离与信息交换产品（网闸）、反垃圾邮件产品、网络综合审计系统、网络脆弱性扫描产品、安全数据库系统、网站恢复产品（硬件）。

6.3.3 澄清、说明或补正

（1）对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，评标委员会应在“政采云”平台发布电子澄清函，要求供应商在平台设置的时间内作出必要的澄清、说明或者补正。供应商在“政采云”平台接收到电子澄清函后根据澄清函内容直接在线编辑或上传 PDF 格式回函，电子澄清答复函使用 CA 证书加盖单位电子签章后提交至评标委员会。供应商的澄清、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。供应商未在规定时间内进行澄清、说明或者补正的，按无效投标处理。

（2）异常情况处理：如遇无法正常使用线上发送澄清函的情况，将以书面形式执行。评标委员会以书面形式要求供应商在规定时间内作出必要的澄清、说明或者补正。供应商的澄清、说明或者补正必须采用书面形式，并加盖公章或者由法定代表人或者其授权的代表签字。

6.3.4 报价修正

（1）报价出现前后不一致的，按照下列规定修正：

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；

②大写金额和小写金额不一致的，以大写金额为准；

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；

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。

同时出现两种以上不一致的，按照上述①-④顺序修正。修正后的报价按照上述“6.3.3 澄清、说明或补正”的规定经供应商确认后产生约束力，供应商不确认的，其投标无效。

（2）评标委员会认为供应商的报价明显低于其他通过符合性审查供应商的报价，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交相关书面证明材料；评标委员会可以要求供应商就提供货物的主要成本、销售费用、管理费用、财务费用、履约费用、计划利润、税金及附加等成本构成事项进行详细陈述。书面证明应当按照上述“6.3.3 澄清、说明或补正”的规定提交。供应商未按规定提交或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）经供应商确认修正后的报价若超过采购预算金额或者最高限价，其投标文件作无效投标处理。

（4）经供应产确认修正后的报价作为签订合同的依据，并以此报价计算价格分。

6.3.5 相同品牌认定

（1）单一产品采购项目，不同供应商提供的产品品牌相同时，按以下规定确定相同品牌的投标有效性。

①采用综合评分法的采购项目，提供相同品牌产品且通过资格审查、符合性审查的不同供应商参加同一合同项下投标的，按一家供应商计算，评审后得分最高的同品牌供应商获得中标人推荐资格；评审得分相同的，由采购人或者采购人委托评标委员会按照招标文件规定的方式确定一个供应商获得中标人推荐资格，招标文件未规定的采取随机抽取方式确定，其他同品牌供应商不作为中标候选人。

②采用最低评标价法的采购项目，提供相同品牌产品的不同供应商参加同一合同项下投标的，以其中通过资格审查、符合性审查且报价最低的参加评标；报价相同的，由采购人或者采购人委托评标委员会按照招标文件规定的方式确定一个参加评标的供应商，招标文件未规定的采取随机抽取方式确定，其他投标无效。

（2）非单一产品采购项目，采购人应当确定核心产品，并在招标文件中载明。不同供应商提供的核心产品品牌相同的，按上述规定处理。核心产品在第二章采购需求规定。

6.3.6 串通投标认定

评标委员会须根据以下规定认定供应商是否有串通投标的行为。

（1）根据《关于防治政府采购招标中串通投标行为的通知》（桂财采[2016]42 号）规定，出现下述情况的，相关供应商的投标作无效投标处理。

①单位负责人为同一人或者存在直接控股、管理关系，参加同一合同项下政府采购活动的不同供应商。

②授权给供应商后参加同一合同项（分标、分包）投标的生产厂商。

③视为或被认定为串通投标的相关供应商。

（2）根据《关于防治政府采购招标中串通投标行为的通知》（桂财采[2016]42 号）规定，有下列情形之一的视为供应商相互串通投标，投标文件将被视为无效。

①不同供应商的投标文件由同一单位或者个人编制；或不同供应商报名的 IP 地址一致的；

②不同供应商委托同一单位或者个人办理投标事宜；

③不同的供应商的投标文件载明的项目管理员为同一个人；

④不同供应商的投标文件异常一致或投标报价呈规律性差异；

⑤不同供应商的投标文件相互混装；

⑥不同供应商的保证金从同一单位或者个人账户转出。

（3）根据《关于防治政府采购招标中串通投标行为的通知》（桂财采[2016]42 号）规定，供应商有下列情形之一的，属于恶意串通行为，投标文件将被视为无效。

①供应商直接或者间接从采购人或者采购代理机构处获得其他供应商的相关信息并修改其投标文件或者响应文件；

②供应商按照采购人或者采购代理机构的授意撤换、修改投标文件或者响应文件;；

③供应商之间协商报价、技术方案等投标文件或者响应文件的实质性内容；

④属于同一集团、协会、商会等组织成员的供应商按照该组织要求协同参加政府采购活动；

⑤供应商之间事先约定一致抬高或者压低投标报价，或者在招标项目中事先约定轮流以高价位或者低价位中标，或者事先约定由某一特定供应商中标，然后再参加投标；

⑥供应商之间商定部分供应商放弃参加政府采购活动或者放弃中标；

⑦供应商与采购人或者采购代理机构之间、供应商相互之间，为谋求特定供应商中标或者排斥其他供应商的其他串通行为。

6.3.7 投标无效认定

（1）在评审过程中如发现下列情形之一的，投标文件将被视为无效：

①投标文件存在法律、法规及监督部门有关文件规定的无效情形。

②投标文件存在招标文件规定的无效情形。

（2）根据财库《关于促进政府采购公平竞争优化营商环境的通知》（〔2019〕38 号）以及《广西壮族自治区财政厅转发财政部关于促进政府采购公平竞争优化营商环境的通知》（桂财采〔2019〕41 号）规定，评标委员会不得因装订、纸张、文件排序等非实质性的格式、形式问题认定投标无效或否决投标，从而限制和影响供应商投标（响应）。

6.3.8 比较与评价

（1）评标委员会按招标文件中规定的评审方法和标准，对符合性审查合格的投标文件进行综合比较与评价。

（2）评标委员会各成员独立对每个有效供应商的投标文件进行评价。评价有误的应及时进行修正。评分标准如有客观分定义，评标委员会所有成员的客观分评分分值应当一致。

（3）评标委员会按综合评分由高到低的排列顺序推荐综合评分排名第一的为第一中标候选人。若中标候选人综合评分相同的，按投标报价由低到高顺序排列；综合评分且投标报价相同的并列；中标候选人并列的，按技术部分得分由高到低顺序排列，若综合评分、投标报价、技术部分均相同的，按商务部分得分由高到低顺序排列。

（4）评标委员会根据评审记录及评审结果编写评审报告，评标委员会成员均应当在评审报告上签字，对自己的评审意见承担法律责任。评审报告签署前，经复核发现存在以下情形之一的，评标委员会应当当场修改评审结果，并在评审报告中记载；评审报告签署后，采购人或者采购代理机构发现存在以下情形之一的，应当组织原评标委员会进行重新评审。

分值汇总计算错误的；分项评分超出评分标准范围的；评标委员会成员对客观评审因素评分不一致的；经评标委员会认定评分畸高、畸低的。

6.4 确定中标人

6.4.1 采购代理机构将在评审结束后 2 个工作日内将评审报告送采购人，采购人在 5 个工作日内按照评审报告中推荐的中标候选供应商顺序确定中标人。

6.4.2 采购人、采购代理机构认为供应商对采购过程、中标结果提出的质疑成立且影响或者可能影响中标结果的，合格供应商符合法定数量时，可以从合格的中标候选人中另行确定中标人的，应当依法另行确定中标人；否则应当重新开展采购活动。

6.5 结果公告

6.5.1 自中标人确定后 2 个工作日内，采购代理机构按照供应商须知前附表的规定公告中标结果。

6.5.2 在发布结果公告的同时，采购代理机构以供应商须知前附表规定的形式向中标人发出中标通知书。中标通知书发出后，采购人改变中标结果，或者中标人放弃中标，应当承担相应的法律责任。

6.5.3 在发布结果公告的同时，采购代理机构以供应商须知前附表规定的形式向未中标人发出招标结果通知书，供应商自行承担未及时查收的后果。

6.6 废标

6.6.1 出现下列情形之一，将导致项目废标：

（1）符合专业条件的供应商或者对招标文件做实质性响应的供应商不足三家；

（2）出现影响采购公正的违法、违规行为的；

（3）供应商的报价均超过了采购预算，采购人不能支付的；

（4）因发生重大变故或采购任务取消的。

6.6.2 废标后采购代理机构将发布废标公告通知供应商。

7．签订合同

7.1 合同授予标准

合同将授予被确定实质上响应招标文件要求，具备履行合同能力，综合评分排名第一的供应商。在中标通知书发出前或签订合同前，如果中标人的组织机构、经营、财务状况发生较大变化，可能造成不能履行合同、无法按照招标文件要求提交履约保证金等情形，不符合中标条件或不满足供应商资格条件要求 ，应在中标通知书发出前或签订合同前及时书面告知采购人，未主动告知，给采购人造成损失的，采购人有权取消其中标资格并没收投标保证金。

7.2 签订合同

7.2.1 如招标文件无特别规定，中标人按招标文件确定的事项签订政府采购合同。

7.2.2 政府采购合同应当包括采购人与中标人的名称和住所、标的、数量、质量、价款或者报酬、履行期限及地点和方式、验收要求、违约责任、解决争议的方法等内容。招标文件、中标人的投标文件及澄清文件等，均为签订政府采购合同的依据。

7.2.3 如中标人不按中标通知书的规定签订合同，其投标保证金将不予退还，并报由同级政府采购监督管理部门处理。

7.2.4 中标人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候选人名单排序，确

定下一候选人为中标人，也可以重新开展政府采购活动。

7.3 合同公告

7.3.1 如招标文件无特殊规定，中标人应在签订合同后 1 个工作日内，将政府采购合同副本送采购代理机构存档。

7.3.2 采购人应当自政府采购合同签订之日起 2 个工作日内，将政府采购合同在省级以上人民政府财政部门指定的媒体上公告，但政府采购合同中涉及国家秘密、商业秘密的内容除外。

7.4 履行合同

7.4.1 采购人与中标人签订合同后，政府采购合同的履行、违约责任和解决争议的方法等适用《中华人民共和国民法典》。合同双方应严格执行合同条款，履行合同规定的义务，保证合同的顺利完成。双方均不得擅自变更、中止或者终止政府采购合同。

7.5 履约验收

7.5.1 采购人可以根据政府采购项目具体情况自行组织验收，或者委托政府采购代理机构、国家认可的质量检测机构开展采购项目履约验收工作。

7.5.2 验收结果合格的，中标人可向采购人申请办理履约保证金（如有）的退付手续；验收结果不合格的，履约保证金（如有）将不予退还，并按合同约定处理，还可能会报告本项目同级财政部门并按照政府采购法律法规及有关规定给予行政处罚或者以失信行为记入诚信档案。

7.5.3 采购合同项目完成验收后，采购人应当将验收原始记录、验收书等资料作为该采购项目档案妥善保管，不得伪造、变造、隐匿或者销毁，验收资料保存期为采购结束之日起至少保存 15 年。

7.5.4 本项目将严格按照本招标文件及合同有关规定进行合同履约验收。招标文件或合同未规定的按财政部关于进一步加强政府采购需求和履约验收管理的指导意见（财库〔2016〕205 号）以及《广西壮族自治区政府采购项目履约验收管理办法》（桂财采〔2015〕22 号）的规定执行。

8．质疑和投诉

8.1 质疑

8.1.1 质疑内容、时限

（1）供应商对政府采购活动有疑问的，可以向采购人或采购代理机构提出询问。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。

（2）供应商为认为招标文件、采购过程、中标或者成交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 7 个工作日内向采购人或采购代理机构提出质疑。采购人或采购代理机构在收到供应商书面质疑后 7 个工作日内，对质疑内容作出答复。

8.1.2 质疑形式

质疑应当采用供应商须知前附表所规定的形式，质疑书应明确阐述招标文件、采购过程或中标结果中使自己合法权益受到损害的实质性内容，提供相关事实、依据和证据及其来源或线索，便于有关单位调查、答复和处理。

8.1.3 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：

（1） 供应商的姓名或者名称、地址、邮编、联系人及联系电话；

（2） 质疑项目的名称、编号；

（3） 具体、明确的质疑事项和与质疑事项相关的请求；

（4） 事实依据；

（5） 必要的法律依据；

（6） 提出质疑的日期。

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。

8.2 投诉

8.2.1 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时间内答复的，可在答复期满后 15 个工作日内按有关规定，向同级财政部门投诉。

8.2.2 投诉书应使用财政部发布的政府采购供应投诉书范本，并应按照“投诉书制作说明”进行编写。

9．其他事项

9.1 代理服务收费由采购代理机构向中标人收取。签订合同前，中标人应向采购代理机构一次付清代理服务费。

9.2 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：

（1）电子交易平台发生故障而无法登录访问的；

（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；

（3）电子交易平台发现严重安全漏洞，有潜在泄密危险的；

（4）病毒发作导致不能进行正常操作的；

（5）其他无法保证电子交易的公平、公正和安全的情况。

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；影响或可能影响采购公平、公正性的，经采购代理机构确认后，应当重新采购。采购代理机构必须对原有的资料及信息作出妥善保密处理，并报财政部门备案。

9.3 本项目的附件及图纸详见供应商须知前附表。

9.4 本项目的其他事项详见供应商须知前附表。

10．其他说明

10.1 其余未尽事宜按《中华人民共和国政府采购法》、《中华人民共和国政府采购法实施条例》的相关规定执行。

10.2 本招标文件是根据国家有关法律及有关政策、法规和参照国际惯例编制，解释权属采购代理机构。

第四章　评审方法及标准

一、评标方法

1、评标方法

本项目采用综合评分法进行评标。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标因素的量化指标评标得分最高的供应商为中标候选人的评标方法。

2、评标依据

评标委员会以招标文件、补充文件、投标文件、澄清及答复为评标依据。

3、评标委员会

本项目评标委员会由政府采购评审专家和采购人代表组成。评标委员会必须公平、公正、客观，不带任何倾向性和启发性；不得向外界透露任何与评审有关的内容；任何单位和个人不得干扰、影响评审的正常进行；评标委员会及有关工作人员不得私下与供应商接触。评审专家发现本人与参加采购活动的供应商有利害关系的，应当主动提出回避。

二、评标程序

1、初步评审：初步评审包括资格检查及符合性检查。

2、澄清（如需要）。

3、详细评审。

4、推荐中标候选人。

三、特别说明：

1、注意事项：本项目实行电子投标，供应商应准备电子投标文件。

2、电子投标文件按政采云平台要求及本招标文件要求制作、加密并递交。具体操作流程可参考《政府采购项目电子交易管理操作指南-供应商》，指南可在“http://www.ccgp-guangxi.gov.cn/PurchaseAdvisory/ImportantNotice/2866753.html”下载。

3、供应商提供的以下相关证明材料属于“必须提供”的文件应加盖供应商公章（CA 签章）/自然人签字或加盖个人 CA 签章，否则投标无效。

4、投标文件（电子响应文件），其中电子投标文件中所须加盖公章部分均采用 CA 签章。若招标文件中有专门标注的某关联点，并要求供应商在电子投标系统中作出响应的，如供应商未对关联点进行响应或者在投标文件其它内容进行描述，造成电子评审不能查询的责任由供应商自行承担。

5、招标文件要求法定代表人（负责人）或委托代理人签字的部分必须签字然后扫描或者拍照做成 pdf 格式上传（或加盖个人 CA 签章），无签字的视为投标无效。

6、电子投标文件中须加盖供应商公章部分均采用 CA 签章，并根据“政府采购项目电子交易管理操作指南-供应商”及本招标文件规定的格式和顺序编制电子投标文件并进行关联定位，以便评审小组在评审时，点击评分项可直接定位到该评分项内容。如对招标文件的某项要求，供应商的电子投标文件未能关联定位提供相应的内容与其对应，则评审小组在评审时如做出对供应商不利的评审由供应商自行承担。电子投标文件如内容不完整、编排混乱导致投标文件被误读、 漏读，或者在按招标文件规定的部位查找不到相关内容的，由供应商自行承担。

7、供应商法人（负责人）或授权代表持有政采云个人 CA 签章的，应在投标文件中涉及到签字的

位置使用个人 CA 签章，没有办理政采云个人 CA 签章的可在投标文件中涉及到签字的位置手写签字后扫描或者拍照做成 PDF 的格式上传即可。

8、投标文件不得涂改，若有修改错漏处，须法定代表人（负责人）或授权委托人签字（或个人 CA 签章）。投标文件因字迹潦草或表达不清所引起的后果由供应商负责。

9、本项目实行网上评审，采用电子投标文件；若供应商参与投标，自行承担投标一切费用。各供应商在截标前应确保成为政采云平台正式注册入库供应商，并完成 CA 数字证书申领。因未注册入库、未办理 CA 数字证书等原因造成无法投标或投标失败等后果由供应商自行承担。供应商将政采云电子交易客户端下载、安装完成后，可通过账号密码或 CA 登录客户端进行投标文件制作。客户端请至网站下载专区查看，如有问题可拨打政采云客户服务热线 95763 进行咨询。

10、供应商进行电子投标应安装客户端软件，并按照采购文件和电子交易平台的要求编制并加密投标文件。供应商未按规定加密的投标文件，电子交易平台将拒收。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。如有特殊情况，采购代理机构延长截止时间和开标时间，采购代理机构和供应商的权利和义务将受到新的截止时间和开标时间的约束。

四、评标内容

1、资格审查

采购人代表对所有供应商的投标文件进行资格审查。以确定供应商是否具备投标资格。资格审查表如下，缺少任何一项或有任何一项不合格者，其资格审查视为不合格。

1.1 供应商具备有效的“营业执照”或“事业单位法人证书”或“自然人的身份证明”副本复印件。

供应商是企业则审查营业执照（副本）复印件；供应商是事业单位，则审查事业单位法人证书（副本）复印件；供应商是非企业专业服务机构的，则审查执业许可证等证明文件复印件；供应商是个体工商户，则审查个体工商户营业执照复印件；供应商是自然人，则审查自然人身份证明复印件；如供应商不是以上所列的法人、组织、自然人的，则提供国家规定的相关证明材料。

1.2 供应商 2022 年度财务状况报告（表）复印件或 2023 年银行出具的资信证明复印件。对于从取得营业执照时间起到投标文件递交截止时间为止不足 1 年的供应商，只需提交投标文件递交截止时间前一个月的财务状况报告（表）复印件。

1.3①投标截止时间前 6 个月内，供应商任意 1 个月依法缴纳税费证明复印件。②投标截止时间前 6 个月内，供应商任意 1 个月的社保缴费证明记录复印件。供应商成立不足 1 个月的，无须提供缴纳税费证明及社保缴费证明。依法免税或不需要缴纳社会保障资金的供应商，须提供相应文件证明其依法免税或不需要缴纳社会保障资金。

1.4 审查无重大违法记录声明。须提供，格式见第六章投标文件格式“投标声明书”。一旦发现供应商提供的投标声明书不实时，则按照《政府采购法》有关提供虚假材料的规定给予处罚。

1.5 诚信要求：①审核标准：供应商如被列入失信被执行人、重大税收违法失信主体、政府采购严重违法失信行为记录名单，则资格审查不予通过，其投标被否决。

②信用信息查询渠道：中国政府采购网“政府采购严重违法失信行为记录名单”信用中国网：“失信被执行人”、“重大税收违法失信主体”

③查询方式：资格审查时，采购人或采购代理机构通过上述渠道查询供应商的信用记录供评委审核。

④信用信息查询记录和证据留存的具体方式：通过上述查询渠道查询的供应商信用记录查询结果，将作为政府采购活动档案留存。

1.6 供应商不得参加资格性审查的情形：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，不得参加本项目同一合同项下的政府采购活动。为本项目提供整体设计、规范编制或者项目管理、监理、检测等服务的供应商，不得再参加本项目的采购活动。

2、符合性检查

资格审查结束后，由评标委员会对通过资格审查的供应商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。符合性检查表如下，缺少任何一项或有任何一项不合格者，其符合性检查视为不合格。

2.1 有效性审查

2.1.1 投标文件签署：投标文件上法定代表人或其授权代表人已按要求签字盖章。

2.1.2 法定代表人身份证明及授权委托书：供应商无授权代表时审查：法定代表人身份证明及附件，格式及附件见第六章投标文件格式要求；供应商有授权代表时审查：法定代表人授权委托书及附件，格式及附件见第六章投标文件格式要求；法定代表人身份证明及授权委托书须有效，符合招标文件规定的格式，签字或盖章齐全。

2.1.3 投标文件或者投标报价唯一性：同一供应商不得提交两个以上不同的投标文件或者投标报价，但招标文件要求提交备选投标的除外。

2.1.4 投标报价：报价超出采购预算金额或最高限价（如有）的，否决其投标。提交选择性报价的，否决其投标。

2.2 完整性审查

对招标文件的响应程度审查：（1）实质性条款响应：对招标文件中所有标注▲号的实质性条款要求响应均无负偏离。（2）投标有效期：满足招标文件规定。

3、串通投标的认定

评标委员会须根据以下规定评审供应商是否有串通投标的行为，并按规定判定投标是否有效。

（1）根据桂财采[2016]42 号《关于防治政府采购招标中串通投标行为的通知》规定，出现下述情况的，相关供应商的投标作无效投标处理。

①单位负责人为同一人或者存在直接控股、管理关系，参加同一合同项下政府采购活动的不同供应商。

②授权给供应商后参加同一合同项（分标、分包）投标的生产厂商。

③视为或被认定为串通投标的相关供应商。

（2）根据桂财采[2016]42 号《关于防治政府采购招标中串通投标行为的通知》规定，有下列情形之一的视为供应商相互串通投标，投标文件将被视为无效。

①不同供应商的投标文件由同一单位或者个人编制；

②不同供应商委托同一单位或者个人办理投标事宜；

③不同的供应商的投标文件载明的项目管理员为同一个人；

④不同供应商的投标文件异常一致或投标报价呈规律性差异；

⑤不同供应商的投标文件相互混装；

（3）根据桂财采[2016]42 号《关于防治政府采购招标中串通投标行为的通知》规定，供应商有下列情形之一的，属于恶意串通行为，投标文件将被视为无效。

①供应商直接或者间接从采购人或者采购代理机构处获得其他供应商的相关信息并修改其投标文件或者响应文件；

②供应商按照采购人或者采购代理机构的授意撤换、修改投标文件或者响应文件;；

③供应商之间协商报价、技术方案等投标文件或者响应文件的实质性内容；

④属于同一集团、协会、商会等组织成员的供应商按照该组织要求协同参加政府采购活动；

⑤供应商之间事先约定一致抬高或者压低投标报价，或者在招标项目中事先约定轮流以高价位或者低价位中标，或者事先约定由某一特定供应商中标，然后再参加投标；

⑥供应商之间商定部分供应商放弃参加政府采购活动或者放弃中标；

⑦供应商与采购人或者采购代理机构之间、供应商相互之间，为谋求特定供应商中标或者排斥其他供应商的其他串通行为。

4、投标有效性的认定

（1）资格审查时，如发现下列情形之一的，投标文件将被视为无效：

①不具备招标文件中规定的资格要求的；

②投标文件签署（签名）、盖章不符合招标文件要求的；

（2）在符合性审查、商务和技术评估时，如发现下列情形之一的，投标文件将被视为无效：

①投标文件未按招标文件要求签署、盖章的；

②投标文件未按招标文件要求提供第六章要求“必须提供”的内容的；

③报价超过招标文件中规定的预算金额或者最高限价的；

④投标文件含有采购人不能接受的附加条件的；

⑤评审过程中发现投标文件中提供虚假材料的；

⑥法律、法规和招标文件规定的其他无效情形。

（3）根据财库〔2019〕38 号《关于促进政府采购公平竞争优化营商环境的通知》以及桂财采〔2019〕41 号 《广西壮族自治区财政厅转发财政部关于促进政府采购公平竞争优化营商环境的通知》规定，评标委员会认定投标有效性时不得因装订、纸张、文件排序等非实质性的格式、形式问题否决投标，从而限制和影响供应商投标（响应）。

5、澄清、说明或补正

对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，评标委员会可要求供应商在合理时间内通过在线询标、电话、电子邮件或传真等不见面、不接触的方式作出必要的澄清、说明或者纠正。内容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。逾期未做澄清、说明或者纠正的，经电话催告仍不澄清的，视为放弃。

6、报价修正

投标文件报价如果出现计算或表达上的错误，修正错误的原则如下：

（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；

（2）大写金额和小写金额不一致的，以大写金额为准；

（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；

（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。

同时出现两种以上不一致的，按照上述顺序修正。修正后的报价按照上述“7、澄清、说明或补正”的规定经供应商确认后产生约束力，供应商不确认的，其投标无效。

7、过低报价合理性的审查

评标委员会认为供应商的报价明显低于其他通过符合性审查供应商的报价，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并提交相关证明材料；评标委员会可以要求供应商就提供货物的主要成本、销售费用、管理费用、财务费用、履约费用、计划利润、税金及附加等成本构成事项进行详细陈述。书面说明应当按照上述“7、澄清、说明或补正”的规定经供应商确认后提交给评标委员会。供应商未按规定提供说明或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。

报价合理性书面说明应当有签字或盖章确认，供应商为法人的，由其法定代表人或者授权代表签名或盖章确认；供应商为其他组织的，由其主要负责人或者授权代表签名或盖章确认；供应商为自然人的，由其本人或者授权代表签名或盖章确认。

8、商务和技术评估、综合比较与评价

评标委员会按招标文件中规定的评标方法和标准，对资格审查和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。具体评标标准见《评分表》。

评标委员会各成员独立对每个有效供应商的投标文件进行评价、打分，然后由评标组长组织评标委员会对各成员打分情况进行核查及复核，评分有误的，应及时进行修正。评标标准如有主客观分定义，评标委员会所有成员的客观分打分分数应当一致。

复核后，评标委员会汇总每个供应商每项评分因素的得分。评标结果汇总完成后，除下列情形外，任何人不得修改评标结果：（1）分值汇总计算错误的；（2）分项评分超出评分标准范围的；（3）评标委员会成员对客观评审因素评分不一致的；（4）经评标委员会认定评分畸高、畸低的。评标报告签署前，经复核发现存在以上情形之一的，评标委员会应当当场修改评标结果，并在评标报告中记载；评标报告签署后，采购人或者采购代理机构发现存在以上情形之一的，应当组织原评标委员会进行重新评审。

9、中标候选人推荐原则

按评标后得分由高到低的排列顺序推荐综合得分排名第一的为第一中标候选人。若中标候选人综合得分相同的，按投标报价由低到高顺序排列；综合得分且投标报价相同的，由采购人按技术分得分由高到低顺序排列，若综合得分、投标报价、技术分均相同的，按系统功能及联动能力分得分由高到低顺序排列。

10、评标争议处理

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。

五、评标标准

（1）投标报价分

序号	类型	评分标准	分值权重	说明
1	投标报价分	以满足招标文件要求且投标价格最低的投标报价为评审基准价，其价格分为满分。其他供应商的价格分统一按照下列公式计算：投标报价得分=（评审基准价/投标报价）×30。	30	如有价格扣除时，投标报价分均按供应商实际投标报价进行价格扣除后的价格进行计算，最终中标金额＝投标报价。价格扣除计算方法见后。

注：政策性扣除计算方法

供应商投标报价将按相应比例进行扣除，用扣除后的价格参与评审（计算价格分），价格扣除比例分别如下：

独立投标	供应商均为所列企业之一（小型企业、微型企业、残疾人福利企业、监狱企业）	价格扣除响应报价的 20%
联合体或分包	小微企业承接的金额比例为 100%	价格扣除响应报价的 20%
	小微企业承接的金额比例达到合同总金额 30%以上	价格扣除响应报价的 4%
注：未提供《中小企业声明函》、《分包意向协议书》或《联合体协议书》或不符合条件的，不享受价格扣除优惠。		

（2）技术及商务资信分

序号	评标因素及分值	分值属性	评标标准	说明
1	技术分（15 分）	客观分	供应商应按招标文件要求提交有效证明的材料。其中招标文件采购需求中标注“★”项的参数为本次采购重要参数条款，无标识的参数为一般性参数条款。 **（1）无标识的技术参数评分（5 分）：** 一档（0 分）：无标识的技术参数有 3 项（含）以上负偏离得 0 分。 二档（1 分）：无标识的技术参数有 2 项负偏离得 1 分。 三档（3 分）：无标识的技术参数有 1 项负偏离得 3 分。 四档（5 分）：无标识的技术参数无负偏离得 5 分。 **（2）标注“★”的技术参数评分（10 分）：**	标注“▲”为实质性条款，有 1 条不满足视为无效投标。如供应商投标文件对招标文件技术要求响应为无偏离，但经评标委员会认定为负偏离的，评标委员会可给

			一档（0 分）：标注“★”的技术参数有 2 项（含）以上负偏离得 0 分。 二档（5 分）：标注“★”的技术参数有 1 项负偏离得 5 分。 三档（10 分）：标注“★”的技术参数无负偏离得 10 分。	予相应档次定档。
2	系统功能及联动能力分（15 分）	客观分	1、序号 4 产品终端安全管理系统，终端安全联动能力：为了简便运维，要求终端安全管理系统支持与本项目网络准入认证系统在同一管理后台进行维护配置管理。终端安全管理系统支持联动安装零信任客户端、可以自定义零信任客户端菜单名称、支持使用零信任认证信息自动登陆。要求提供在线功能演示，满足得 3 分。 2、序号 9 产品威胁感知系统：为提升医院对未知威胁的快速处置能力，要求威胁感知系统支持基于入侵检测规则、威胁情报的旁路阻断功能。支持根据时间段、IP、域名等条件配置阻断黑名单、阻断白名单。支持配置观察模式，仅记录不阻断。要求提供在线功能演示，满足得 4 分。 3、序号 15 产品网闸：为保障医院数据库数据同步安全，要求网闸具备数据库数据防泄漏能力，可对数据库字段进行敏感信息脱敏过滤，支持正则表达式、关键字、枚举、数值区间、时间区间等方式来匹配关键字段内容，支持替换成指定内容进行数据脱敏。要求提供在线功能演示，满足得 4 分。 4、序号 17 产品零信任（可信访问控制台），零信任系统联动能力：为提升系统安全，要求零信任系统支持与本项目服务器安全管理系统联动，实现更加安全的自身防护能力。要求提供在线功能演示，满足得 4 分。 注：以上功能需要在线功能演示予以佐证。供应商提供的在线功能演示可以以搭建的系统平台方式进行在线操作演示，也可以采用平台演示视频录像文件方式进行在线演示。	未演示或不符合演示要求得 0 分。
3	安全服务方案	主观分	一档（4 分）：安全服务方案简单，内容基本完整，	须提供对本项目

	分（13 分）		方法措施一般，提供≥3 名以上的安全服务工程师； 二档（8 分）：安全服务方案比较合理，内容较完整，方法措施较可行，能简单掌握网络安全建设的架构、安全现状。具有质量保障措施方案。供应商或本项目安全服务厂商应具备广西本地化的技术支撑能力，提供≥5 名以上具备注册信息安全工程师（CISE）或注册渗透测试工程师（CISP-PTE）资质认证的服务工程师，提供≥1 名同时具备注册渗透测试专家(CISP-PTS)认证证书和 Web 应用安全专家（CWASP）认证证书的安全服务专家。供≥1 名项目经理，项目经理同时具备项目管理、企业架构师、云安全认证、CISP 注册信息安全专业人员认证证书。供应商或安全服务厂商须具备在线威胁分析工具，实现威胁情报样本的批量与自动化检测。深度分析能力不少于以下 6 个维度：IOC 自动化数据流检测、失陷情报批量查询、样本哈希批量查询、样本自动化分析、恶意 IP 批量查询、邮件批量自动化检测等；（提供威胁分析工具官网链接及官网界面截图证明） 三档（13 分）：安全服务方案总体评述细致、可行，完全满足采购文件要求。熟悉采购人的网络安全建设的架构、安全现状，能准确把握采购人对网络安全建设的需求。组织机构和人员配备有针对性，项目执行和保障措施详细可行。供应商或本项目安全服务厂商应具备广西本地化的技术支撑能力，提供≥10 名以上具备注册信息安全工程师（CISE）或注册渗透测试工程师（CISP-PTE）资质认证的服务工程师，提供≥1 名同时具备注册渗透测试专家(CISP-PTS)认证证书和Web应用安全专家（CWASP）认证证书的安全服务专家。提供≥1 名项目经理，项目经理同时具备项目管理、企业架构师、云安全认证、CISP 注册信息安全专业人员认证证书。供应商或安全服务厂商须具备在线威胁分析工具，实现威胁情报样本的批量与自动化检测。深度分析能力不少于以下 8 个维度：IOC 自动化数据流检测、失陷情报批量查询、样本哈希批量查询、样本自动化分	安全服务方案与安全服务人员证书、社保证明，未提供的得0分。

			析、恶意 IP 批量查询、APT 样本自动化检测器、PCAP 自动化分析、邮件批量自动化检测等；（提供威胁分析工具官网链接及官网界面截图证明） 注：以上安全服务人员、项目经理必须是供应商或本项目安全服务厂商的正式员工，提供相关人员的资质证书复印件和开标前半年内任意 1 个月份的社保证明复印件附于投标文件中。	
4	项目实施与售后服务方案（6 分）	主观分	一档（2 分）：本项目的实施方案比较简单，措施不够具体。售后服务方案一般，有售后服务承诺、售后服务流程。配备 1 名售后应急响应支持人员以支撑突发网络安全事件的应急响应处置。 二档（4 分）：对本项目的总体方案比较详细，措施得当、进度计划可行。售后服务方案较好，有该项目详细的系统建设的售后服务方案及培训计划、售后服务流程等。配备 1 名售后应急响应支持人员以支撑突发网络安全事件的应急响应处置。应急响应支持人员需具备攻防渗透能力，持有 CISP-PTE 或同等国家级渗透测试能力证书。 三档（6 分）：对本项目的总体方案详细具体，措施具有针对性、进度计划可行，具备质量控制措施、总体项目实施方案的可操作性强。售后服务方案良好，有该项目详细的系统建设的售后服务方案及培训计划，售后服务流程，故障响应时间优于招标文件等。配备 1 名广西本地化的售后应急响应支持人员以支撑突发网络安全事件的应急响应处置。应急响应支持人员需具备攻防渗透能力和应急响应能力，同时持有 CISP-PTE 及 CCSRP（网络与信息安全应急人员认证）或同等国家级渗透测试、应急响应能力证书。 注：应急响应支持人员须是供应商或本项目安全服务厂商的正式员工，提供相关人员的资质证书复印件和开标前半年内任意 1 个月份的社保证明复印件附于投标文件中。	须提供售后服务方案，未提供的得 0 分。

5	信誉及履约能力分（21 分）	客观分	1、供应商或本项目威胁感知系统生产厂商在近 6 个月在国家信息安全漏洞共享平台（CNVD）成员单位漏洞报送数量月度排名中，获得前三名 5-6 次得 5 分，获得前三名 3-4 次得 2 分，得前三名 1-2 次得 1 分，没有得 0 分。（提供 CNVD 官网漏洞信息月度通报截图及链接证明，加盖供应商公章） 2、供应商或本项目威胁感知系统生产厂商拥有漏洞研究的专业团队，历年来发现了大量的安全漏洞并报告厂商修复，自 2019 年以来所提交的漏洞数大于 250 个得 5 分，150-250 个得 2 分，150 个以下得 1 分，没有得 0 分。（提供官网截图及链接证明，加盖供应商公章）。 3、供应商或本项目威胁感知系统生产厂商拥有全国性的漏洞响应平台，累计报告 100 万个以上漏洞，并汇聚 10 万个以上的白帽专家。满足得 5 分。（提供平台官网截图、官网链接以及漏洞响应平台软著复印件证明，加盖供应商公章）。 4、本项目威胁感知系统生产厂商具备中国合格评定国家认可委员会（CNAS）认可的机构颁发的 ISO22301 业务连续性管理体系、ISO27701 隐私信息管理体系。满足其中一项认证得 3 分，全部满足得 6 分。（提供证书复印件，加盖供应商公章）	

（3）综合评分

分项	投标报价得分	技术及商务资信分	总分
分值	30	70	100
综合评分=投标报价得分+技术及商务资信分（注：各项评分分值计算保留小数点后两位，小数点后第三位“四舍五入”）			

4.1 偏离认定说明

供应商根据采购需求中技术参数为基准，填写响应表，对于响应表或证明材料与技术参数不符的，按如下规定：

（1）实质性参数要求提交证明材料的，证明材料没有体现响应表中响应的内容的或未提供证明材料的，视为无效响应。非实质性参数要求提交证明材料的，证明材料没有体现响应表中响应的内容的或未提供证明材料的，视为负偏离。

（2）响应表中响应的内容与证明材料不一致的，以证明材料为准作为评审依据。

（3）同时出现以上两种情况的，按照（1）-（2）顺序认定。

（4）响应表与采购需求中技术参数比较有漏项的，如为实质性参数漏项，视为未响应；如为非实质性参数漏项，视为负偏离。

（5）一项技术参数有多条小项要求的，必须全部响应。如只响应部分参数，视为漏项，按照（4）判定。评审时以每一条技术参数为评审依据。

（6）对于区间涵盖值参数，例：电压“测量范围 3V-5V”，同时满足下限值更低及上限值更高才视为正偏离，例：响应为“测量范围 2V-6V”。如有一端负偏离，不管另一端如何，均视为负偏离，例：响应为“测量范围 4V-6V”。

（7）对于区间任意值参数，例“5mm≤间距≤10mm”或“间距 7.5±2.5mm”，若间距响应值为 5mm-10mm 中任意区间值或任意一个数值（含本数）时为无偏离，例：“6mm≤间距≤8mm”、“8±2mm”、“8mm”。超过区间范围视为负偏离，例：“3mm≤间距≤12mm”、“8±4mm”、“3-12mm”、“3mm”。此类参数不存在正偏离。

（8）对于单边任意参数的要求，例“长度≥50cm”，若响应为 50 cm 及 50cm 以上任意一个数值，均视为无偏离；若响应小于 50cm，视为负偏离。此类参数无正偏离。

（9）对于固定参数，响应与采购需求中技术参数一致，视为无偏离，其他均视为负偏离，此类参数无正偏离。

（10）如采购需求中技术参数有特殊要求与上述说明不一致的，以特殊要求为准。

第五章　合同主要条款格式

合同编号：

采购项目名称：

采购单位（甲方）：桂林医学院附属医院　　采购计划号：_____

供 应 商（乙方）：_____　　项 目 编 号 ： _____

签　订　地　点：桂林医学院附属医院　　签 订 时 间; _____

根据《中华人民共和国政府采购法》、《中华人民共和国民法典》等法律、法规规定，按照招投标文件（采购文件）规定条款和中标（成交）供应商承诺，甲乙双方签订本合同。

第一条　合同标的

1、项目一览表。

序号	货物或服务名称	数量及单位	单价（元）	总价（元）
……				
服 务 期 限 :				
投 标 总 报 价 ： 人 民 币 大 写　　元 整 （ ¥　　）				

本次报价包含服务交付成果、设计、组织、策划、开发、调研、技术协助、校准、培训、技术指导、产品价、运输费（含装卸费）、保险费、安装调试费、税费、产品检测费、产品质保期内维护费等类似服务内容的全部费用。对于本文件中明确列明必须报价的货物或服务，乙方应分别报价。对于本文件中未列明，而乙方认为必需的费用也需列入总报价。在合同实施时，甲方将不予支付乙方没有列入的项目费用，并认为此项目的费用已包括在投标总报价中。

第二条　质量保证

乙方所提供的服务及服务内容必须与投标文件承诺相一致，有国家强制性标准的，还必须符合国家强制性标准的规定，没有国家强制性标准但有其他强制性标准的，必须符合其他强制性标准的规定。

第三条　权利保证

1、乙方应保证所提供服务在使用时不会侵犯任何第三方的专利权、商标权、著作权等知识产权及其他合法权利，且所有权、处分权等没有受到任何限制。

2、没有甲方事先书面同意，乙方不得将由甲方提供的有关合同或者任何合同条文、规格、计划、图纸、样品或者资料提供给与履行本合同无关的任何其他人。即使向履行本合同有关的人员提供，也应注意保密并限于履行合同的必需范围。乙方的保密义务持续有效，不因为本合同履行终止、解除或者无效而解除。

第四条　服务期限、服务地点及其他

1、服务期限：_____，服务地点：_____。

2、乙方应按投标文件的承诺向甲方提供相应的服务，并提供所服务内容的相关技术资料。

3、乙方提供不符合投标文件和本合同规定的服务成果，甲方有权拒绝接受。

4、乙方完成服务后应及时书面通知甲方进行验收，甲方应在收到通知后七个工作日内开始验收。验收合格后由甲乙双方签署验收单并加盖采购人公章，甲乙双方各执一份。

5、甲乙双方应按照《广西壮族自治区政府采购项目履约验收管理办法》、双方合同、投标文件验收。

6、甲方在初步验收或者最终验收过程中如发现乙方提供的服务成果不满足投标文件及本合同规定的，可暂缓向乙方付款，直到乙方及时完善并提交相应的服务成果且经甲方验收合格后，方可办理付款。

7、甲方验收时以书面形式提出异议的，乙方应自收到甲方书面异议后五个工作日内及时予以解决，否则甲方有权不出具服务验收合格单。乙方未按照上述约定时间内解决或经甲方判定无法解决的，甲方有权解除合同，乙方应当按照合同总额的 30%支付违约金。

第五条　付款方式

合同签订后 5 个工作日内支付合同总额 30%的预付款；按照等保三级要求部署，并且顺利通过三级等保测评， 支付合同总金额 30%的项目款；全部部署完成，调试无误，设备整体验收，顺利通过攻防演练（不被攻破），经甲方验收合格并签发验收合格单后支付总金额 20%；下一年顺利通过攻防演练（不被攻破）， 支付余下合同总额 20% (无息)。甲方付款前，乙方应向甲方开具符合甲方要求的正规财务票据，否则甲方有权暂缓或拒付款项且不构成违约。

第六条　税费

本合同执行中相关的一切税费均由乙方负担，合同另有约定的除外。

第七条　违约责任

1、除不可抗力原因外，乙方没有按照合同规定的时间提供服务的，甲方可要求乙方支付违约金。每推迟一天按合同金额的 3‰支付违约金，该违约金累计不超过合同金额的 10%。超过合同约定时间 5 日的，甲方有权解除合同，乙方应当按照合同总额的 30%支付违约金。

2、乙方提供的服务如侵犯了第三方合法权益而引发的任何纠纷或者诉讼，均由乙方负责交涉并承担全部责任。如导致甲方被追索或主张责任的，甲方有权解除合同，乙方应当退还甲方已支付的费用，并按照合同总金额的 30%支付违约金给甲方。

3、乙方完成本合同项下的服务未通过验收合格的，经整改 3 次仍未通过验收合格的，视为乙方不能完成本合同项下义务，甲方有权解除合同，乙方应当退还甲方已支付的费用，并按照合同总金额的30%支付违约金给甲方。

4、因乙方的行为造成违约或乙方无法按照合同约定提供相应服务，甲方有权解除合同或者继续履行合同，乙方还应承担甲方为维护权利而支付的律师费、诉讼费、保全费、保险费、鉴定费等费用。

第八条　不可抗力事件处理

1、在合同有效期内，任何一方因不可抗力事件导致不能履行合同，则合同履行期可延长，其延长期与不可抗力影响期相同。

2、不可抗力事件发生后，应立即通知对方，并寄送有关权威机构出具的证明。

3、不可抗力事件延续一百二十天以上，双方应通过友好协商，确定是否继续履行合同。

第九条　合同争议解决

1、因服务质量问题发生争议的，应邀请国家认可的质量检测机构进行鉴定。服务符合标准的，鉴定费由甲方承担；服务不符合标准的，鉴定费由乙方承担。

2、因履行本合同引起的或者与本合同有关的争议，甲乙双方应首先通过友好协商解决，如果协商不能解决，可向甲方所在地有管辖权人民法院提起诉讼。

3、诉讼期间，本合同继续履行。

第十条　合同生效及其它

1、合同经双方法定代表人或者授权代表签字并加盖单位公章后生效（委托代理人签字的需后附授权委托书，格式自拟）。

2、合同执行中涉及采购资金和采购内容修改或者补充的，须经财政部门审批，并签书面补充协议报财政部门备案，方可作为主合同不可分割的一部分。

3、本合同未尽事宜，遵照《中华人民共和国民法典》有关条文执行。

第十一条　本合同记载地址视为送达地址，送达地址变更需采用书面形式。

本合同尾部载明的乙方地址及联系人用于接收往来函件及诉讼法律文书，且适用于因本合同履行相关的一切纠纷处理程序（如仲裁、诉讼、执行等）的送达。如有变更，乙方需以书面方式通知甲方，未书面通知变更的，凡向合同记载地址或联系方式、联系人发送的文件及信息，无论是否实际收到，均视为有效送达 。

第十二条、本合同一式七份，甲方执伍份，乙方执一份，代理机构执一份。本合同经甲乙双方签字盖章后生效，补充协议含售后服务承诺书等，与本合同具有同等法律效力。如甲乙双方合同条款内容不一致者，以在甲方存档者为正本。

第十三条、本合同如有未尽事宜，甲乙双方另行协商。

附件 1：本项目设备（系统）配置清单

序号	部件编号	名称	规格型号	单位	数量	分项价格（元）	备注

1							

附件 2：售后服务承诺书[原则上须有生产厂家或省级（含省级）以上代理商的盖章**]。**

附件 3：供应商的营业执照。

甲方（章） 桂林医学院附属医院 年 月 日	乙方（章） 年 月 日
单位地址：桂林市秀峰区乐群路 15 号	单位地址：
法定代表人：	法定代表人：
委托代理人：	委托代理人
电话：0773-2802050 招标办	电话：
电子邮箱：	电子邮箱：
开户银行：	开户银行：
账号：	账号：
邮政编码：	邮政编码：

医疗卫生机构医药产品廉洁购销合同

甲方（医疗卫生机构）：桂林医学院附属医院

乙方（医药生产经营企业及其代理人）：

为进一步加强医疗卫生行风建设，规范医疗卫生机构医药购销行为，有效防范商业贿赂行为，营造公平交易、诚实守信的购销环境，经甲、乙双方协商，同意签订本合同，并共同遵守：

一、甲乙双方按照《民法典》及医药产品购销合同约定购销药品、医用设备、医用耗材试剂等医药产品。

二、甲方应当严格执行医药产品购销合同验收、入库制度，对采购医药产品及发票进行查验，不得违反有关规定合同外采购、违价采购或从非规定渠道采购。

三、甲方严禁接受乙方以任何名义、形式给予的回扣，不得将接受捐赠资助与采购挂钩。甲方工作人员不得参加乙方安排并支付费用的营业性娱乐场所的娱乐活动，不得以任何形式向乙方索要现金、有价证券、支付凭证和贵重礼品等。被迫接受乙方给予的钱物，应予退还，无法退还的，有责任如实向有关纪检监察部门反映情况。

四、严禁甲方工作人员利用任何途径和方式，为乙方统计医师个人及临床科室有关医药产品用量信息，或为乙方统计提供便利。

五、乙方不得以回扣、宴请等方式影响甲方工作人员采购或使用医药产品的选择权，不得在学术活动中提供旅游、超标准支付食宿费用。

六、乙方指定_____作为销售代表洽谈业务。销售代表必须在工作时间到甲方指定地点联系商谈，不得到住院部、门诊部、医技科室等推销医药产品，不得借故到甲方相关领导、部门负责人及相关工作人员家中访谈并提供任何好处费。

七、乙方如违反本合同，一经发现，甲方有权终止购销合同，并向有关卫生计生行政部门报告。如乙方被列入商业贿赂不良记录，则按照《国家卫生计生委关于建立医药购销领域商业贿赂不良记录的规定》（国卫法制发[2013]50 号）相关规定处理。

八、本合同作为医药产品购销合同的重要组成部分，与购销合同一并执行，具有同等的法律效力。

九、本合同一式七份，甲方执伍份，乙方执一份，代理机构执一份，并从签订之日起生效。

甲方（盖章）：桂林医学院附属医院　　**乙方（盖章）：**

法定代表人（负责人）：　　**法定代表人（负责人）：**

经办人签名：　　**经办人签名：**

年　月　日　　**年　月　日**

合同附件 2

履约验收方案

1.履约验收工作参加人员

1.1 履约验收主体单位

采购人（如委托第三方机构签订，应注明收费方式）

1.2 履约验收参加人员

采购人代表、委托机构代表、成交供应商代表及采购人邀请的其他人员

2.履约验收时间

20XX 年 XX 月 XX 日

3.履约验收地点

XX 市 XX 区 XX 路 XX 号

4.履约验收方式

采购人自行验收

5.履约验收程序

5.1 成立验收小组

5.2 量化验收标准

5.3 组织验收

5.4 出具验收报告

5.5 验收结果公告

5.6 验收资料归档

采购合同项目完成验收后，采购人整理好验收原始记录、验收书等资料后妥善保管，不得变造、隐匿或者销毁，验收资料保存期为采购结束之日起至少保存 15 年。

6.履约验收内容

6.1 商务验收内容

对采购标的交付的情况、财务和服务要求，包括交付（实施）的时间（期限）和地点（范围），付款条件（进度和方式），包装和运输，售后服务，保险等进行验收。

6.2 技术验收内容

对采购标的的功能和质量要求，包括性能、材料、结构、外观、安全，或者服务内容和标准等进行验收。

7.履约验收标准

验收标准：

（1）中标（成交）供应商应提供完备的技术或服务资料、装箱单和合格证等，并派遣专业人员进行现场安装调试。验收合格条件如下：

服务技术参数与响应文件中响应表或证明材料一致，性能或指标达到规定的标准。否则，以实际服务技术参数与响应文件响应表参数或证明材料比较，按如下情况处理：

①供应商响应文件响应表或证明材料中满足或优于的技术参数，在验收时实际不满足技术参数要求的，视为供应商违约，采购人有权终止合同拒收服务成果，并追究供应商责任，同时报财政部门备案。

②供应商响应文件响应表或证明材料中优于的技术参数，在验收时实际仅满足并未优于技术参数要求的，视为供应商违约，采购人有权终止合同拒收服务成果，并追究供应商责任，同时报财政部门备案。

③供应商响应文件响应表或证明材料中不满足的技术参数，在验收时实际满足技术参数的要求，以满足技术参数的要求验收。

④供应商响应文件响应表或证明材料中满足的技术参数，在验收时实际优于技术参数的要求，以满足技术参数的要求验收。

⑤供应商响应文件响应表或证明材料中优于的技术参数，在验收时实际也优于技术参数的要求，但没有达到响应表或证明材料中优于的程度，由采购人与供应商协商按是否满足要求验收。

（1）在测试或试运行期间所出现的问题得到解决，并运行或工作正常。

（2）在规定时间内完成交付及验收，并经采购人确认。

（3）服务在安装调试并试运行符合要求后，才作为最终验收。

（4）成交供应商提供的服务未达到招标文件规定要求，且对采购人造成损失的，由成交供应商承担一切责任，并赔偿所造成的损失。

（5）政府采购合同约定的其他要求及投标文件响应的其他标准。

8.履约验收其他事项

无

广西壮族自治区政府采购项目合同验收书

根据政府采购项目（采购合同编号：GXZC20XX-XX-XXXXX-JDZB）的约定，我单位对（XXXX 采购项目）政府采购项目中标（或成交）供应商 XX 公司（填写供应商名称）提供的服务（或工程、货物）进行了验收，验收情况如下：

<table>
<tr><td colspan="2">验收方式：</td><td colspan="3">□自行验收　　□委托验收</td></tr>
<tr><td>序号</td><td>名　称</td><td>服务内容、标准等</td><td>数量</td><td>金　额</td></tr>
<tr><td>1</td><td>XXXX 设备</td><td></td><td>1 套</td><td>¥0.00 元</td></tr>
<tr><td colspan="3">合　计</td><td></td><td>¥0.00 元</td></tr>
<tr><td colspan="5">合计大写金额：人民币元整</td></tr>
<tr><td>实际交付日期</td><td colspan="2">20　年　月　日</td><td>合同交付验收日期</td><td>20　年　月　日</td></tr>
<tr><td>验收具体内容</td><td colspan="4">中标人所提供服务的内容满足采购合同约定的要求、标准。</td></tr>
<tr><td rowspan="2">验收小组意见</td><td colspan="4">验收结论性意见：同意（不同意）通过项目验收</td></tr>
<tr><td colspan="4">有异议的意见和说明理由：
签字：</td></tr>
<tr><td colspan="5">验收小组成员签字：</td></tr>
<tr><td colspan="5">监督人员或其他相关人员签字：
或受邀机构的意见（盖章）：</td></tr>
<tr><td colspan="5">中标或者成交供应商负责人签字或盖章：　　受托机构的意见（盖章）：
联系电话：　　年　月　日　　联系电话：　　年　月　日
采购人签字或盖章：
联系电话：　　年　月　日</td></tr>
</table>

备注：本报告单一式 4 份（采购单位 1 份、供应商 1 份、采购监督部门备案 1 份、采购代理机构 1 份）

第六章　投标文件格式

注：有签字、盖章要求的应按要求签字（签章）、盖章（签章）。

1．投标文件封面参考格式（资格证明文件）：

电子投标文件

资格证明文件

项目名称：

项目编号：

分标号：（若无留空或写“/”）

供应商名称：

供应商地址：

年　月　日

目录

（应有页码）

1．投标声明书格式：

投标声明书

致：*（采购人名称）*：

*（供应商名称）*系中华人民共和国合法企业，*（经营地址）*。

我*（姓名）*系*（供应商名称）*的法定代表人，我方愿意参加贵方组织的*（项目名称）*项目的投标，为便于贵方公正、择优地确定中标人及其投标产品和服务，我方就本次投标有关事项郑重声明如下：

（1）我方向贵方提交的所有投标文件、资料都是准确的和真实的。

（2）我方不是采购人的附属机构；也不是为本项目提供整体设计、规范编制或者项目管理、监理、检测等服务的供应商或其附属机构。

（3）我方承诺在参加本政府采购项目活动前，没有被纳入政府部门或银行认定的失信名单，我方具有良好的商业信誉。

（4）我方及本人承诺在参加本政府采购项目活动前三年内，在经营活动中没有重大违法记录及不良信用记录。重大违法记录是指供供应商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。如我方提供的声明不实，则自愿承担《政府采购法》有关提供虚假材料的规定给予的处罚。

（5）我方承诺具有履行本项目合同所必需的设备和专业技术能力。

（6）我方承诺未被列入失信被执行人、重大税收违法失信主体、政府采购严重违法失信行为记录名单，如我方提供的声明不实，则接受本次投标作为否决投标的处理，并根据财库〔2016〕125 号《财政部关于在政府采购活动中查询及使用信用记录有关问题的通知》规定接受失信联合惩戒。

（7）我方承诺中标后按规定缴纳代理服务费。如未按时缴纳，贵方可不退还我方提交的投标保证金，并从中扣除代理服务费。

我方对以上声明负全部法律责任。如有虚假或隐瞒，我方愿意承担一切后果，并不再寻求任何旨在减轻或免除法律责任的辩解。

供应商名称（电子签章）：

年　　月　　日

2. 法人或者其他组织的营业执照等证明文件、自然人的身份证明。即供应商是企业则提供营业执照（副本）复印件；供应商是事业单位，则提供事业单位法人证书（副本）复印件；供应商是非企业专业服务机构的，则提供执业许可证等证明文件复印件；供应商是个体工商户，则提供个体工商户营业执照复印件；供应商是自然人，则提供有效的自然人身份证明复印件；如供应商不是以上所列的法人、组织、自然人的，则提供国家规定的相关证明材料。（加盖供应商电子签章）。

3. 财务状况报告（表）复印件或银行出具的资信证明复印件。对于从取得营业执照时间起到截标时间为止不足 1 年的供应商，只需提交截标时间前一个月的财务状况报告（表）复印件。（按“评审方法及标准” “资格审查表”规定提供）。（加盖供应商电子签章）。

4. 依法缴纳税费证明和社会保险缴纳证明材料。供应商成立不足 1 个月的，无须提供缴纳税费证明及社保缴费证明。依法免税或不需要缴纳社会保障资金的供应商，须提供相应文件证明其依法免税或不需要缴纳社会保障资金。（按“评审方法及标准” “资格审查表”规定提供）（加盖供应商电子签章）。

5. 具备法律、行政法规规定的其他要求的证明材料（按“评审方法及标准” “资格审查表”规定提供）。**（如招标文件有要求时提供）**

6. 满足供应商特定资格条件的其他证明材料加盖供应商电子签章（按“评审方法及标准” “资格审查表”“ 供应商应符合的特定资格条件”规定提供）。**（如招标文件有要求时提供）**

6.1 供应商直接控股股东信息表

序号	直接控股股东名称	出资比例	身份证号码或者统一社会信用代码	备注
1				
2				
3				
……				

注：

1.直接控股股东：是指其出资额占有限责任公司资本总额百分之五十以上或者其持有的股份占股份有限公司股份总额百分之五十以上的股东；出资额或者持有股份的比例虽然不足百分之五十，但依其出资额或者持有的股份所享有的表决权已足以对股东会、股东大会的决议产生重大影响的股东。

2.本表所指的控股关系仅限于直接控股关系，不包括间接的控股关系。公司实际控制人与公司之间的关系不属于本表所指的直接控股关系。

3.供应商不存在直接控股股东的，则填“无”。

供应商名称(电子签章)：

日期：　　年　月　　日

6.2 供应商直接管理关系信息表

序号	直接管理关系单位名称	统一社会信用代码	备注
1			
2			
3			
……			

注：

1.管理关系：是指不具有出资持股关系的其他单位之间存在的管理与被管理关系，如一些上下级关系的事业单位和团体组织。

2.本表所指的管理关系仅限于直接管理关系，不包括间接的管理关系。

3.供应商不存在直接管理关系的，则填“无”。

供应商名称(电子签章)：

日期：　年　月　日

7．供应商认为应当要提交的其他资格证明材料。

2．投标文件封面参考格式（商务技术文件）：

电子投标文件

商务技术文件

项目名称：

项目编号：

分标号：（若无留空或写“/”）

供应商名称：

供应商地址：

年　月　日

目录

（应有页码）

1．法定代表人身份证明（**无授权代表时提供**）：

法定代表人身份证明

供应商名称：_____

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：_____；身份证：_____

系_____（ 供应商名称）的法定代表人。

特此证明。

供应商名称(电子签章)：_____

年　　月　　日

附件：法定代表人身份证复印件

1．授权委托书（有授权代表时提供）：

法定代表人授权委托书

致：*（采购人名称）*：

我*（法定代表人姓名）*系*（供应商名称）*的法定代表人，现授权委托本单位在职职工（姓名）以我方的名义参加*（项目名称）*项目的投标活动，并代表我方全权办理针对上述项目的投标、开标、评审、签约等具体事务和签署相关文件。

我方对被授权人的签名事项负全部责任。

在撤销授权的书面通知以前，本授权书一直有效。被授权人在授权书有效期内签署的所有文件不因授权的撤销而失效。

被授权人无转委托权，特此委托。

被授权人签字或签章：_____　　法定代表人签字或签章：_____

职务：_____　　职务：_____

被授权人身份证号码：_____　　授权人身份证号码：_____

被授权人手机号码及邮箱：

供应商名称(电子签章)：_____

年　　月　　日

附件：法定代表人身份证复印件及授权代表身份证复印件

第一部分 商务文件

（本商务文件供应商可自行编写，也可参照下述提纲编写）

1．对本项目第二章《采购需求》“商务要求”的响应表：

序号	招标文件的商务要求	投标文件响应内容	偏离说明
	……		

注：（1）本表应对招标文件第二章《采购需求》中所列商务要求进行响应，并根据响应情况在“偏离说明”栏填写正偏离或负偏离及原因，完全符合的填写“无偏离”。

（2）第二章《采购需求》中的总体要求无需响应。

（3）偏离认定说明详见评审方法及标准。

（4）本表可扩展。

供应商名称(电子签章)：_____ 日 期：_____

2．售后服务机构概况

售后服务机构名称			
地址			
注册资本金		其中：供应商出资比例	
员工总人数		其中：技术人员数	
经营期限			
售后服务协议			
售后服务内容			
工作业绩			
服务承诺			
业务咨询电话		传 真	
负责人		联系电话	

供应商名称(电子签章)：_____ 年 月 日

3．售后服务方案（如有，供应商自行编写）

4．近年供应商类似成功案例的业绩证明（附中标书或合同复印件）。

类似成功案例业绩一览表

序号	甲方单位名称	项目名称或服务内容	服务周期或时间（年/月）	团队人数	合同总价（元）	采购单位联系人及联系电话

注：

（1）未附证明材料的业绩无效，证明材料见第四章《评审方法及标准》规定

（2）类似项目的定义见第四章《评审方法及标准》规定。

（3）本表可拓展。

供应商名称(电子签章)：_____　　年　　月　　日

5．供应商认为需提供的其他材料（根据招标文件编写）

6. 无串标行为承诺函

供应商参加本项目无围标串标行为的承诺函

一、我方承诺无下列相互串通投标的情形：

1.不同供应商的投标文件由同一单位或者个人编制；或者不同供应商报名的 IP 地址一致的；

2.不同供应商委托同一单位或者个人办理投标事宜；

3.不同的供应商的投标文件载明的项目管理员为同一个人；

4.不同供应商的投标文件异常一致或者投标报价呈规律性差异；

5.不同供应商的投标文件相互混装；

6.不同供应商的投标保证金从同一单位或者个人账户转出。

二、我方承诺无下列恶意串通的情形：

1.供应商直接或者间接从采购人或者采购代理机构处获得其他供应商的相关信息并修改其投标文件或者投标文件；

2.供应商按照采购人或者采购代理机构的授意撤换、修改投标文件或者投标文件；

3.供应商之间协商报价、技术方案等投标文件或者投标文件的实质性内容；

4.属于同一集团、协会、商会等组织成员的供应商按照该组织要求协同参加政府采购活动；

5.供应商之间事先约定一致抬高或者压低投标报价，或者在招标项目中事先约定轮流以高价位或者低价位中标，或者事先约定由某一特定供应商中标，然后再参加投标；

6.供应商之间商定部分供应商放弃参加政府采购活动或者放弃中标；

7.供应商与采购人或者采购代理机构之间、供应商相互之间，为谋求特定供应商中标或者排斥其他供应商的其他串通行为。

以上情形一经核查属实，我方愿意承担一切后果，并不再寻求任何旨在减轻或者免除法律责任的辩解。

供应商名称(电子签章)：

日期：　年　月　日

第二部分 技术文件

（本技术文件供应商可自行编写，也可参照下述提纲编写）

1．对本项目第二章《采购需求》技术要求的响应表

序号	招标文件要求（注明章节及条款号）	投标文件响应内容	偏离说明
……			
……			

注：（1）本表应对招标文件第二章《采购需求》中所列技术要求进行响应，并根据响应情况在“偏离说明”栏填写正偏离或负偏离及原因，完全符合的填写“无偏离”。
（2）第二章《采购需求》中的总体要求无需响应。
（3）偏离认定说明详见评审方法及标准。
（4）本表可扩展。

供应商名称(电子签章)：_____ 日 期：_____

2．项目拟投入服务团队人员结构表（包括但不限于学历、证书情况、职称、年龄等）

项目拟投入服务团队人员（含项目负责人）一览表

姓名	职务	分配岗位	持证情况	年龄	劳动合同编号

注：在填写时，如本表格不适合投标单位的实际情况，可根据本表格式自行划表填写。

供应商名称(电子签章)：_____ 日 期：_____

3．安全服务方案（如有，供应商自行编写）

4.项目实施与售后服务方案（如有，供应商自行编写）

5.信誉及履约能力相关证明材料（如有，供应商自行编写）

6．为本项目提供的其他优惠服务。（如有，供应商自行编写）

7．供应商需要说明的其他文件和说明。（如有，供应商自行编写）

3．投标文件封面参考格式（报价文件）：

电子投标文件

报价文件

项目名称：

项目编号：

分标号：（若无留空或写“/”）

供应商名称：

供应商地址：

年　月　日

第三部分 报价文件

1．投标函格式：

投 标 函

致：_*（采购人名称）*_：

我方已仔细研究了*（项目名称）*的招标文件的全部内容。签字代表*（授权代表姓名）*经正式授权并代表供应商_*（供应商名称）*提交投标文件。

据此函，签字代表宣布同意如下：

（1）我方已详细审查全部“招标文件”，包括修改文件（如有的话）以及全部参考资料和有关附件，已经了解我方对于招标文件、采购过程、采购结果有依法进行询问、质疑、投诉的权利及相关渠道和要求。

（2）我方在投标之前已经与贵方进行了充分的沟通，完全理解并接受招标文件的各项规定和要求，对招标文件的合理性、合法性不再有异议。

（3）本投标有效期自投标截止之日起_____天。

（4）如中标，本投标文件至本项目合同履行完毕止均保持有效，我方将按“招标文件”及政府采购法律、法规的规定履行合同责任和义务，并承诺不分包及转包他人。

（5）我方同意按照贵方要求提供与投标有关的一切数据或资料。

（6）与本项目有关的一切正式往来信函请寄：

地址：_____邮编：_____ 电话：_____

传真：_____

供应商代表姓名_____ 职务：_____邮箱：_____

供应商名称(电子签章)：

日期：_____年____月___日

2．投标报价明细表格式：

投标报价明细表

金额单位：人民币（元）

序号	货物或服务名称	报价	备注
	……		
服务期限：			
投标总报价：人民币大写　　元整（¥　　）			

注：本表如与政采云平台不一致的，以政采云平台为准。

供应商名称（电子签章）：

日　期：　　年　月　日

3．过低报价合理性的说明。（如有）

评标委员会认为供应商的报价明显低于其他通过符合性审查供应商报价的，供应商将被要求以书面方式提供说明。为避免在评审现场因未能及时提供说明而导致被评标委员会作为无效投标，供应商自行决定是否直接在此处进行陈述。格式自拟。（具体要求详见第四章评审方法及标准“过低报价合理性的审查”）

4．其他文书格式

4.1 符合小型、微型企业政府采购政策证明材料。（非小型、微型企业无需提供）。

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，提供的货物全部由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（招标文件中明确的所属行业）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（招标文件中明确的所属行业）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（电子签章）：　　日期：

注：

（1）标的名称按照第二章项目采购需求的货物名称填写，所属行业标明“/”的，无需在上表填写。

（2）如供应商为联合体或分包的，声明函中“项目名称”应填写联合体中小微企业承担的具体内容或者小微企业具体分包内容。

（3）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参照国务院批准的中小企业划分标准，根据企业自身情况如实判断。

（4）根据工业和信息化部对“从业人员”定义的答复，《民法典》、《公司法》等法律规定，分公司不具有法人资格，其民事责任由总公司承担。企业划型时，应将分公司的从业人员、营业收入、资产总额等指标数据纳入合并计算。

（5）根据国际统计局《劳动工资统计报表制度》，从业人员数是指本单位工作，并取得工资活其他形式劳动报酬的人员数，是在岗职工、劳务派遣人员及其他从业人员之和。

（6）本声明函由供应商填写，供应商应按中小企业划分标准《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 号以及《金融业企业划型标准规定》（银发〔2015〕309 号））判断是否为中小企业。

（7）供应商对《中小企业声明函》的真实性负责，如有虚假则需承担不利后果。依法享受中小企业优惠政策的，采购人或采购代理机构在公告成交结果时，同时公告其《中小企业声明函》，接受社会监督。

（8）上述企业属于大企业的分支机构或控股股东为大企业或与大企业的负责人为同一人的，不得享受价格扣除优惠政策。接受分包的小微企业与分包企业之间存在直接控股、管理关系的，不得享受价格扣除优惠政策。

4.2 监狱企业须提供最新一期《XX 省监狱企业产品目录》或其他监狱企业证明材料。（非监狱企业无需提供）

4.3 残疾人福利性单位须提供《残疾人福利性单位声明函》，格式如下。（非残疾人福利性单位无需提供）

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（（CA 签章））：

日　期：

5. 开标一览表

格式详见政采云平台，且仅在政采云平台填写即可。