**扬州大学附属医院****信息化提升工程一期**

**云资源与云安全租赁项目竞争性磋商文件**

## 一、项目基本情况

1.项目名称：扬州大学附属医院信息化提升工程一期云资源与云安全租赁项目

2.采购方式：竞争性磋商

## 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，并提供下列材料：
1.1法人或者其他组织的营业执照等证明文件**(复印件加盖供应商公章)**；
1.2 若法定代表人参加询价的，须提供本人身份证复印件**(原件备查)；**若授权代表参加的，须提供《法人授权书》原件和授权代表身份证复印件**（原件备查）**；银行、保险、石油石化、电力、电信等有行业特殊情况的，取得营业执照的分支机构可以分公司名义参与投标，招标文件中涉及的“法定代表人”在前述特殊行业中即对应为“分支机构负责人”。

1.3 依法缴纳职工社会保障资金的证明材料**(复印件加盖供应商公章)**(税务、银行或社会保险基金管理部门出具的2022年6月-2022年8月近三个月内任意一个月缴纳职工社会保障资金的缴款凭证或缴款证明)；

1.4 供应商2022年6月-2022年8月近三个月内任意一个月依法纳税的缴款凭证**(复印件加盖供应商公章)；**

1.5 与第（1.4）条相对应的纳税申报表或经会计师事务所审计的2021年度财务报告（成立不满一年不需提供）**(复印件加盖供应商公章)**；
 1.6 参加本次政府采购活动前3年内在经营活动中没有重大违法记录的书面声明**(原件）；**

1.7 供应商信用承诺书**(原件)**；
1.8 供应商未被“信用中国”网站（www.creditchina.gov.cn）、“中国政府采购网"网站 (www.ccgp.gov.cn)列入失信被执行人、重大税收违法案件当事人名单、政府采购严重违法失信行为记录名单**（是否被列入失信名单的查询结果将以网页打印的形式加盖供应商公章）**；

2.本项目的特定资格要求：

无

## 三、获取竞争性磋商文件

1、时间：2022年9月2日至 2022年9月8日（北京时间）

2、地点：扬州市邗江中路368号扬州大学附属医院采购中心

3、联系人、电话：张老师 0514-82981199-80465

## 四、提交投标文件截止时间、开标时间和地点

1、时间： 2022年9月9日15点00分（北京时间）

2、地点：扬州大学附属医院行政楼407会议室

## 五、其他补充事宜

1、投标文件制作份数要求：一式伍份（壹份正本、肆份副本）。每份投标文件须清楚标明“正本”或“副本”字样。一旦正本和副本不符，以正本为准。

2、本次招标投标保证金：本项目不收取保证金。

3、疫情防控期间注意事项：

疫情防控期间，凡参加投标的相关人员应在投标截止时间前，完成以下程序:

(一)投标人授权委派人员不得超过1人并且该授权委托人应递交投标人出具的授权委托书和24小时核酸检测阴性报告;

(二)投标人授权委派人员递交投标文件时，应同时递交具有其本人签名的承诺书:本人承诺14天内未接触过“新冠肺炎”确诊或疑似病例，未接触过疫情重点地区人员，未与确诊、疑似病例和疫情重点地区人员有聚餐、聚会、大型会议、其他大型活动等密切接触史，如存在隐瞒上述情况，本人依法承担相应法律责任;

 (三)参加投标、评标的相关人员应自行佩戴口罩及其他必备的防护用具;

(四)投标的相关人员进入投标现场后，应在开标室等候并与其他人员保持1米以上距离，不得随意走动;

(五)上述要求至国家疫情防控下发最新通知废止。

**供应商须知**

（一） 响应文件的组成：

1.响应函（格式见附件）

2.资格声明（格式见附件）

3.资格证明文件：

3.1法人或者其他组织的营业执照等证明文件**(复印件加盖供应商公章)**；
3.2 若法定代表人参加调研的，须提供本人身份证复印件**(原件备查)；**若授权代表参加的，须提供《法人授权书》原件和授权代表身份证复印件**（原件备查）**；

3.3 依法缴纳职工社会保障资金的证明材料**(复印件加盖供应商公章)**(税务、银行或社会保险基金管理部门出具的2022年6月-2022年8月近三个月内任意一个月缴纳职工社会保障资金的缴款凭证或缴款证明)；

3.4 供应商2022年6月-2022年8月近三个月内任意一个月依法纳税的缴款凭证**(复印件加盖供应商公章)；**

3.5 与第（1.4）条相对应的纳税申报表或经会计师事务所审计的2021年度财务报告（成立不满一年不需提供）**(复印件加盖供应商公章)**；
 3.6 参加本次政府采购活动前3年内在经营活动中没有重大违法记录的书面声明**(原件）；**

3.7 供应商信用承诺书**(原件)**；
3.8 供应商未被“信用中国”网站（www.creditchina.gov.cn）、“中国政府采购网"网站 (www.ccgp.gov.cn)列入失信被执行人、重大税收违法案件当事人名单、政府采购严重违法失信行为记录名单**（是否被列入失信名单的查询结果将以网页打印的形式加盖供应商公章）**；

4.本项目的特定资格要求：

无

**上述1-4条必须全部提供，如有遗漏，其整个响应文件无效。**

5. 报价一览表

6. 如有以下文件自拟并自行添加至响应函中：

（1）要求采购人提供的配合；

（2）其它（供应商认为有必要提供的声明和文件）。

（二） 响应文件的要求：

1. 所有文件、往来函件均应使用简体中文（规格、型号辅助符号例外）。

2. 响应文件由供应商按要求参考给定格式如实填写（编写），须有法人（盖章）、法定代表人或被授权代表签字或盖章，方为有效，未尽事宜可自行补充。

3. 一律以人民币为报价结算货币,单位为“元”。

4. 响应文件应用不褪色的墨水书写或打印。

5. 响应文件参考响应函格式中的顺序制作，并请编制目录。由于编排混乱导致响应文件被误读或查找不到，责任由供应商承担。

6. 响应文件份数为正本一份，副本四份，须各自装订成册，并注明“正本”、“副本”字样，密封，同时注明供应商名称。

7. 响应文件不应有涂改、增删和潦草之处，如有必须修改时，修改处必须有法人章、法定代表人或法定代表人被授权代表的签字。

*本项目采用投标文件第一次报价和现场第二次报价的报价方式，第二次报价不得高于第一次报价，****任何有选择的报价(方案)将不予接受。***

（三） 无效响应文件的确认：

供应商有下列情况之一者，其响应文件无效：

1.响应文件未按规定的期限、地点送达的；

2.响应文件未按要求密封、签署、盖章的；

3.不具备采购文件中规定的资格要求或未按采购文件规定的要求提供资格证明文件的；

4.响应文件未按采购文件规定的内容和要求填写的；

5.响应文件中有采购文件未允许提供的选择性内容的；

6.项目总报价超过本项目预算的；

7.提供虚假材料的（包括但不限于工商营业执照、财务报表、资格证明文件等）；

8.不符合法律、法规和采购文件中规定的其他实质性要求的；

9.供应商被“**信用中国**”网站（www.creditchina.gov.cn）、“**中国政府采购网**"(www.ccgp.gov.cn)列入失信被执行人、重大税收违法案件当事人名单、政府采购严重违法失信行为记录名单。

10.其他法律、法规及本谈判文件规定的属非响应性的询价响应文件的情形。

（四） 评审：

评审工作由扬州大学附属医院负责组织。

具体评审事务由依法组建的询价小组负责。

1.响应文件的审查

（1）本项目采用投标文件第一次报价和现场第二次报价的报价方式，第二次报价不得高于第一次报价。大写金额和小写金额不一致的，以大写金额为准；对不同文字文本响应文件的解释发生异议的，以中文文本为准。

（2）正本与副本不符，以正本为准。

2.评审程序

（1）响应文件审核。审核分为资格性检查和符合性检查。

①资格性检查。依据法律法规和采购文件的规定，对响应文件中的资格证明等进行审查，以确定报价供应商是否具备报价资格。

②符合性检查。依据采购文件的规定，从响应文件的有效性、完整性和对采购文件的响应程度进行审查，以确定是否对采购文件的实质性要求作出响应。

（2）澄清有关问题。对响应文件中含义不明确、同类问题表述不一致或者有明显文字和计算错误的内容，询价小组可以书面形式（应当由询价小组专家签字）要求供应商作出必要的澄清、说明或者纠正。供应商的澄清、说明或者补正应当采用书面形式，由其被授权的代表签字。

**项目需求及相关说明**

1. **项目背景**

依据医院信息化建设规划，2021年医院实施“信息化提升工程一期”建设，为满足一期及未来信息化发展需求，现对医院“云资源与云安全”建设内容进行专门规划与建设。本项目以一期云资源应用需求为基本需求，结合未来医院信息化建设需求，构建医院云资源与云安全管理体系。

项目建设应充分体现医疗业务服务的连续性、医疗信息的安全性、政策的合规性等行业特点。

本项目预算价：***40万元（三年服务期总费用），报价时报一年期费用。***

服务期及付款方式：服务期三年，合同一年一签。在年度评分考核合格及双方无异议情况下续签下一年度服务合同。合同采用后付费方式，即年度服务期满，服务质量合格的情况下，凭开具的发票付款。

1. **建设目标**

建设信息化提升工程一期应用项目云资源：依据医院信息化提升工程一期建设内容提供云资资源与云安全管理，满足医院一期云应用部署要求（具体需求见建设内容）。

建设医院云资源与云安全管理体系：构建医院云资源与云安全统一管理体系，充分考虑一期建设需求及未来医院信息化发展对云资源与云安的全管理需要，具备多套安全产品协同、高效资源利用、平滑升级、灵活扩展、部署便捷等性能。

逐步迁移医院原有云资源的应用，实现医院外网、内外网交互等应用的统一安全管理。

满足网络安全等级保护2.0三级（下简称等保三级）、《江苏互联网医院建设标准与规范》、互联网医院申报等信息安全管理要求。

1. **政策依据**

项目建设应满足以下标准

1、《国家健康医疗大数据标准、安全和服务管理办法》国卫规划发〔2018〕23号

2、《互联网医院管理办法（试行）》国卫医发〔2018〕25号

3、《江苏省卫生信息化项目建设网络安全管理规定（试行）》苏卫办规划【2022】2号；

4、《关于做好互联网应用IPv6升级改造工作的通知-江苏省IPv6规模部署升级改造实施指南》扬卫规划函【2022】1号；

5、《信息安全等保护管理办法》、《商用密码应用安全性评估管理办法》等规定；

1. **建设内容**

**1、建设清单**

本次项目云资源与云安全应包括以下内容。

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **序号** | **内容** | **名称** | **配置要求** | **数量** |
| 1 | 互联网应用服务云资源 | 应用服务器（联空） | 4核16G/70G系统盘/200G数据盘/正版操作系统、版本为WindowsServer2019Standard或以上，1年服务，见详细技术指标要求。 | 3 |
| 日志服务器（联空） | 4核8G/70G系统盘/500G数据盘/正版操作系统、版本为WindowsServer2019Standard或以上，1年服务，见详细技术指标要求。 | 1 |
| 数据库服务器（联空） | 8核16G/70G系统盘/500G数据盘（SSD）/正版操作系统、版本为WindowsServer2019Standard或以上，双机热备，1年服务，见详细技术指标要求。 | 2 |
| 平台服务器（内外网转换） | 8核16G/70G系统盘/500G数据盘/正版操作系统、版本为WindowsServer2019Standard或以上，1年服务，见详细技术指标要求。 | 1 |
| 前置服务器（第三方） | 8核16G/70G系统盘/500G数据盘/正版操作系统、版本为WindowsServer2019Standard或以上，1年服务，见详细技术指标要求。 | 1 |
| 负载均衡 | 50M带宽(主备，支持IPV6)，1年服务，见详细技术指标要求。 | 2 |
| 2 | 互联网应用云安全资源（包括但不限于） | 堡垒机 | 用于集中管理资产访问权限，为运维人员提供统一、高效、安全的运维通道，可提供运维身份鉴别、账号管控、系统操作审计等多种功能。1年服务。 | 1 |
| 防火墙 | 云环境下租户网络边界的下一代防火墙，具有统一管理互联网到云业务主机的精细化访问控制、高效威胁防护和高级威胁检测等功能。1年服务。 | 1 |
| 数据库审计 | 针对数据库系统的安全审计产品，对来自应用系统客户端和DBA对数据库的访问行为进行全面审计，对SQL注入、危险操作进行记录和实时预警、及时阻止，从而达到保护数据库的良好效果。1年服务。 | 1 |
| Web网站安全防护 | 对网站或者APP的业务流量进行恶意特征识别及防护，将正常、安全的流量回源到服务器。避免网站服务器被恶意入侵，保障业务的核心数据安全，解决因恶意攻击导致的服务器性能异常问题。具备Web安全防护、DDoS攻击防护、CC防护等。1年服务，见详细技术指标要求。 | 1 |
| SSL证书 | 网站和移动应用（APP）及小程序提供数据HTTPS加密协议访问，保障数据的安全。装载SSL证书产品后自动激活浏览器中显示“锁”型安全标志，地址栏以“https”开头。1年服务，见详细技术指标要求。 | 1 |
| 主机安全 | 主机安全是集防病毒、防火墙、入侵防御于一体的主机安全解决方案，旨在解决虚拟化环境下虚拟主机的病毒风险、攻击风险、管理风险及宿主主机的安全等一系列的安全问题。1年服务，见详细技术指标要求。 | 8 |
| 3 | 线路租用 | 连接院内网络线路 | 可选实体VPN或专线打通医院内网。50Mbps带宽以上，1年服务。 | 1 |
| 4 | 安全服务 | 云资源安全运营服务 | 提供云上业务的安全防护与闭环处置，确保业务的安全、稳定与连续性运营。（1）通过**专职专属服务经理与技术专家团队**提供7\*24小时全年无间断的监测、分析与响应服务；（2）**提供云态势感知平台和威胁狩猎平台服务**包括：①.接入设备情况；②.总体安全评级，并可自定义评级规则；③.业务风险总览、资产风险总览；④.资产感知情况；⑤.热点事件发生情况；（3）**提供业务上线评估服务**，对需要上云部署的业务系统进行资产梳理、漏洞发现等安全风险评估。 | 1 |

**2、详细技术指标要求**

**（1）云服务器资源**

|  |  |
| --- | --- |
| **名称** | **指标参数要求** |
| 云服务器 | 1. 按照配置要求提供不少于8台通用型云服务器
2. 支持基础配置变更，可进行实例的vCPU、内存、系统盘、数据盘等配置的增加和减少
3. 支持IPv4地址协议和配置、支持IPv6地址协议和配置，创建实例时，手动配置内网IP
4. 支持安全组配置，更换实例所在安全组、修改实例所在安全组规则和作用范围
5. 支持实例vCPU、内存、网络、磁盘等全量实例监控
6. 支持快照、镜像、配置安全组策略等基础功能
7. 支持虚拟私有云，可以支持在一个云数据中心中灵活设定多个虚拟私有云，达到端到端的隔离效果
 |
| 负载均衡 | （1）50M带宽，支持IPV6（2）基础架构采用集群部署，保证服务的稳定性（3）会话保持功能：可针对负载均衡服务监听器开启会话保持功能（4）多种协议：支持四层(TCP/UDP)以及七层(HTTP/HTTPS)协议负载，满足不同应用场景需求（5）多种转发策略：支持加权轮询、加权最小连接数、源IP等均衡方式（6）健康检查：支持用户自定义健康检查方式和频率（7）▲支持负载均衡器NAT64虚拟服务根据业务分配调度到不同服务器，提供第三方权威机构关于“负载均衡器NAT64虚拟服务根据业务分配调度到不同服务器”功能项的产品检测报告。 |

**（2）云安全资源**

|  |  |
| --- | --- |
| **名称** | **指标参数要求** |
| 堡垒机 | 1. 可管理设备数量不少于10个，支持运维IPv6地址的主机。
2. 堡垒机支持采用高可用架构部署，保证各项服务正常运维。
3. 详细记录用户登录资源的所有操作，包括：资源名称、协议类型、主机或应用地址、资源账户、起止时间、会话时长、操作用户、来源IP、操作记录、文件传输记录、会话协同记录。
4. 支持对SSH字符命令的审计，并可基于自定义的起止时间、内容关键字、主机IP、用户名、来源IP、会话ID进行搜索。
5. 支持对RDP会话进行审计，并可以基于自定义的起止时间、内容关键字、主机IP、用户名、类型、来源IP、会话ID进行搜索。
6. 支持对文件传输进行审计，并可以基于自定义的起止时间、内容关键字、主机IP、用户名、类型、来源IP、会话ID进行搜索。
7. 所有的会话审计均可通过保存搜索项实现快速查询。
8. 支持从一条命令定位到用户的操作过程；回放过程支持暂停和加速播放操作。
9. 会话录像回放支持跳过空闲时段，支持设置时间类型，时间类型需包括绝对时间和相对时间。

1年租用服务。 |
| 防火墙 | 1. 支持互联网暴露情况分析。
2. 支持云内资源统一外连管控。
3. 具备攻击防护功能，支持基于不同安全区域防御DNSFlood、HTTPFlood攻击，并支持警告、阻断、首包丢弃、TC反弹技术、NS重定向、自动重定向、手工确认等多种防护措施。
4. 具备访问控制功能，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。
5. 支持云内资源主动外连检测与防御。
6. ▲为有效应对勒索病毒攻击，要求提供的防火墙组件具备勒索软件通信防护功能，提供第三方评测机构关于“勒索软件通信防护”的功能检测报告。
7. 支持ECS高危漏洞检查和统计。
8. 支持安全策略的快速检索及基于名称、地址、端口、协议多维度的高级策略检索，支持策略的复制、调序、查询。
9. 支持统计网络内威胁事件的数量及对应的风险等级；支持一键跳转查看详情并自动显示关联日志；可基于网络连接、应用名称、威胁事件处置威胁事件。
10. 支持三权分立管理，权限设置至少包括全部权限，仅具有策略变更权限和仅具有日志审计权限、仅具有账户配置权限、虚系统配置管理权限以及虚系统审计权限；支持以读写、只读、无权限的方式自定义权限管理，权限管理的范围至少包括策略配置、对象配置、网络配置、系统配置、统计分析、威胁处置等。
11. 1年租用服务。
 |
| 数据库审计 | 1. 支持在目标数据库安装agent解决云环境、虚拟化环境内部流量无法镜像场景下数据库的审计。
2. 审计Agent代理运行时CPU占用率低于3%，内存占用小于100M。
3. 支持Oracle、SQLServer、DB2、Informix、Sybase、MySQL等主流数据库审计。
4. 支持PostgreSQL、人大金仓（Kingbase）、达梦（DM）、南大通用数据库（Gbase）、等数据库审计。
5. 支持主流业务协议HTTP审计。（提供截图证明材料）
6. 支持实现对SQLServer（2005及以上版本）数据库采用加密协议通讯的审计。
7. 支持数据库操作表、视图、索引、存储过程等[各种对象的所有SQL操作审计](#_支持各种对象的SQL审计_1)。
8. 支持数据库请求和返回的双向审计，特别是返回字段和结果集、执行状态、返回行数、执行时长、客户端工具、主机名等内容。
9. 支持对SQL注入、跨站脚本攻击等web攻击的识别与告警
10. 可自定义审计规则。
11. 规则各条件之间支持[与或非逻辑](#_支持与或非逻辑关联)关系。
12. 具有丰富的全文检索条件，包括数据库时间段、日期范围、数据库登录账号、客户端工具、数据库操作类型、影响行数等条件的审计查询。
13. 系统内置[多种报表模板库](#_内置多种报表模板)，支持自定义报表。
14. 支持PDF、word等格式的报表导出。
15. 提供审计策略和[系统配置信息的单独导入、导出](#_系统配置单独导入导出)功能。
16. 支持对安全风险进行告警。
17. 采用B/S架构管理。
18. 数据库异常行为审计。
19. ▲支持以时间、源IP、客户端程序、业务系统、数据库用户、数据库名、操作类型、表名、返回行数、影响行数、响应时长、响应码、策略、规则、风险级别、SQL模版为条件的数据库风险查询。 （提供功能截图并加盖厂商公章）。
20. 1年租用服务。
 |
| Web网站安全防护 | （1）业务并发请求峰值：5000QPS（2）防护域名数：提供不少于1个域名（域名为同一备案主体，且包含子域名）的安全防护，二级域名不限，支持扩展。（3）防护端口：包含5个非标准端口配置，可支持除80、443之外的端口，支持扩展（4）▲接入方式：公有云支持CNAME接入，托管云支持A记录解析。（5）▲Web安全防护：包括SQL注入攻击防护、XSS跨站脚本攻击防护、目录遍历攻击防护等功能，为保证防护效果，提供第三方权威机构关于“SQL注入攻击防护、XSS跨站脚本攻击防护、目录遍历攻击防护”功能项的产品检测报告。（6）支持DDoS攻击防护：包含：SYNFlood、ACKFlood、UDPFlood、ICMPFlood等攻击类型的防护（7）支持https防护（8）CC防护：支持默认CC防护规则和自定义CC防护规则（9）防扫描及探测：支持高频Web攻击封禁（可自定义）、目录遍历防护（可自定义）、扫描工具封禁、协同防御（10）、安全域流量审计（11）支持网页防篡改1年租用服务。 |
| SSL证书 | 提供SSL证书（服务端和客户端），且均支持ECC、RSA或SM（国密）三种加密方式。1年租用服务。 |
| 主机安全 | 1. 保护主机数量不少于8个。
2. 采用B/S架构设计，管理控制中心高度集成化，无需额外安装或外接数据库即可实现日志存储和分析展示，无需额外安装或对接升级服务器即可实现文件、特征库的升级和分发
3. 支持查杀病毒木马，勒索软件，挖矿病毒，实时监控进程可疑行为，网站后门，主机异常事件，敏感文件篡改，异常网络连接，异常账号，应用入侵事件。
4. 提供不少于3种病毒查杀引擎，可根据不同虚拟化环境和查杀要求灵活开启与关闭；同时产品应支持利用CPU虚拟化技术提升系统的安全防护能力
5. 内置webshell扫描引擎，针对网站系统恶意webshell、后门等文件进行扫描防护；能够针对webshell文件设定白名单，对文件进行加白处理，避免对核心网站系统文件造成影响
6. 提供快速扫描、全盘扫描、指定扫描等多种扫描防护模式，支持自定义路径、指定引擎、自定义处理动作的个性化扫描防护
7. 支持对主机安全缺陷、配置进行扫描评估，通过打分形式展现不合规和风险程度。能够对windows操作系统上的策略、服务、组件等进行扫描凭，对linux操作系统上的账号、服务、安全参数、进程、配置等进行扫描评估，并给出修复建议，修复建议包括自动修复和手动提示修复
8. 支持对主机的安全加固，针对利用漏洞的恶意软件、程序进行拦截并阻止其在主机上运行，提供软件、程序的黑白名单，以减少对系统程序的误拦截风险，（提供截图证明材料）
9. 支持入侵防御，可对来自网络层的拒绝服务、缓冲区溢出、木马后门、web攻击、恶意网络扫描、恶意入侵提权等各类威胁流量的检测与防护。
10. 支持手动、自动升级系统文件、引擎版本、特征库信息，能够基于分组、时间设定灰度升级策略
11. ▲支持安全策略一体化配置，通过一条策略即可实现不同安全功能的配置，包括：终端病毒查杀的文件扫描配置、文件实时监控的参数配置、WebShell检测的检测和威胁处置方式、暴力破解的威胁处置方式和信任目录，提供第三方权威机构的产品功能检测报告。
12. ▲支持对服务器重要目录进行权限控制，仅允许配置的可信进程操作该目录并提供配置指引；（提供界面截图并加盖厂商公章）

1年租用服务。 |

1. **专线或者vpn**

提供不低于50M带宽1个公网IP，实现云上网络与院内网络内网加密打通，一主一备2条网络专线或其它线路冗余措施，保障网络安全。

1. **安全服务**

|  |  |
| --- | --- |
| **名称** | 技术参数 |
| **安全服务** | 1. 免费提供业务上线评估服务，对需要上云部署的业务系统进行资产梳理、漏洞发现等安全风险评估
2. 提供专属管家服务：提供专属服务经理，可以通过移动电话、微信、QQ、邮件等方式即时响应客户的需求，并7\*24小时全年无中断服务。
3. 问题上报与安全预警：实时监测客户VPC安全基线状态，针对存在安全风险的项通过邮件或IM群实时通告客户并告知解决方案处置措施。如：防火墙暂停服务、开放高危端口至公网、堡垒机未使用、EDR防护策略未开启、主机并发会话瞬时过高等资源及配置优化：提供基于云产品与服务的云资源及配置的优化建议。
4. ▲为保证安全问题发现与闭环处置的准确度，要求提供部署虚拟化态势感知平台和流量检测探针组件，结合云端实时在线的安全值守工程师，实现7\*24小时的安全运营服务，支持使用服务工具支持将收集的安全日志上传到安全服务平台上，并支持在该平台上对服务工具进行管理（需提供组件产品彩页及功能截图，并加盖厂商公章）
5. 资产发现与识别：借助安全工具对用户资产进行全面发现和深度识别，并在后续服务过程中触发资产变更等相关服务流程，确保安全运营中心中资产信息的准确性和全面性。
6. 安全现状评估：包含脆弱性、病毒类事件、攻击行为、失陷类事件等安全现状的评估。
7. 弱口令分析与管理：实现信息化资产不同应用弱口令猜解检测，如：SMB、Mssql、Mysql、Oracle、smtp、VNC、ftp、telnet、ssh、mysql、tomcat等。
8. 漏洞分析与管理：通过漏洞扫描工具识别系统安全漏洞，结合多种信息对识别的漏洞进行优先级排序，最后提出切实可行的漏洞修复指导。同时，借助漏洞跟踪管理平台，可以有效地追踪资产漏洞生命周期，清楚地掌握资产的脆弱性状况，实现漏洞全生命周期的可视、可控和可管。
9. 策略调整：安全专家根据安全事件分析的结果以及处置方式，根据用户授权情况按需对安全组件上的安全策略进行调整工作（需提供用户授权界面截图，并加盖厂商公章）
10. ▲事件管理：针对分析得到的勒索病毒、挖矿病毒、篡改事件、webshell、僵尸网络等安全事件，通过工具和方法对恶意文件、代码进行根除，帮助用户快速恢复业务，消除或减轻影响。（需提供用户授权界面截图，并加盖厂商公章）
11. 安全隐患分析：提供系统级的安全隐患分析服务，包括外部访问、系统维护、资源使用等信息汇总。提供系统安全分析，包括可疑访问、恶意访问、安全试探、异常访问数据分析等安全隐患的预警性分析。每月一份安全分析报告，全年十二份报告，提供报表查看页面。
12. ▲提供漏洞验证服务，针对发现的漏洞进行验证，验证漏洞在已有的安全体系发生的风险及分析发生后可造成的危害。针对已经验证的漏洞，自动生成漏洞工单，安全专家跟进漏洞状态，各个处理进度透明，方便招标方清晰了解当前漏洞的处置状态，将漏洞处理工作可视化（提供服务工具漏洞工单截图，需展示当前漏洞的处置状态，并加盖厂商公章）
13. ▲提供1年安全运营的原厂服务，提供原厂关于7\*24小时安全服务以及原厂管家运维的承诺函。
 |

**五、售后服务要求**

**1、安全服务要求**

投标人应保证业务应用系统的支撑环境，包括但不限于服务器、网络、存储等相关物理环境能满足安全***三级等保***要求，依据招标需求向采购人提供本次项目中所涉及安全服务内容。同时供应商需提供完整、可行的安全防护设计方案。

**2、技术支持与服务要求**

**（1）日常运维服务**

投标人提供专门运维服务团队完成日常运维服务，设立专职人员，由其负责组织和协调采购人处理云平台使用过程中出现的各类问题，包括系统使用、管理、升级和维护。利用监控系统或人工对硬件设备及应用系统的运行情况进行7\*24小时的不间断巡检监控，及时发现安全隐患，包括用户信息检查及帐号安全检查、WEB运行状态实时监控、磁盘空间监控、授权异常异常访问、参数优化、垃圾清理等服务，对发现的问题及时处理并形成监控报告，及时通知采购人。定期开展安全应急演练，提升院内人员服务水平。投标人团队在日常安全运维管理中应包括但不限于以下方面工作：1.组织定期评估网络运行安全风险；2.防范计算机病毒和网络攻击、入侵等危害网络安全行为的防护措施；3.监测、记录网络运行状态、网络安全事件的技术手段，做好安全防护；4.做好网络、数据库操作日志，日志留存不少于六个月。投标人每月形成书面报告报告以上平台运行安全情况，及时处置上级通报以及自我检查发现的网络安全隐患、漏洞和事件，并在规定时间期限内向采购人反馈处置整改情况，实在因第三方因素无法整改的，应具备及时关闭业务；

**（2）故障响应服务**

投标人应当提供高效的系统维护服务，有效防范系统风险，需保持7\*24小时电话畅通，能够在系统发生故障问题时，能够协调人力资源在5分钟内响应，30分钟内解决故障。

（**3）重点保障要求**

为保障业务高峰期内系统平稳运行，缓解系统高峰期内因业务发生量增大而带来系统压力风险，要求供应商根据业务周期性特点，加大运维保障力度，保证在业务高峰期内系统平稳运行。对安全厂商、上级部门的漏扫报告及时进行一对一技术分析与处理，并形成书面报告。

**（4）部署迁移服务**

**采购人因业务与安全服务需要涉及到部分项目的迁移，投标人应根据采购人要求完成系统迁移工作，系统中断时间不得超过3小时，迁移过程中产生的所有费用由投标人承担。**

投标人在建设期除了提供安全云服务外，还需要将医院内网映射在互联网的资产统一扎口管理，包括但不限于打卡小程序、OA、体检信息查询、电子发票、设备管理软件等，以一个二级域名+多个端口+多个路径的模式（举例如http://xxx.aaa.com:80/1/2/3---、https://xxx.aaa.com:443/1/2/3---等）对照映射以上多个业务，支持日志管理记录用户访问、系统运行等完整日志并具备完整性验证功能，协助开通互联网80和443端口并备案；（需要提供完整解决方案和承诺函）

**（5）服务承诺**：1、投标人应签署SLA服务协议承诺，云主机服务可用性≥99.97%，数据库审计服务可用性≥99.97%，堡垒机服务可用性≥99.97%，日志审计服务可用性≥99.97%，下一代防火墙服务可用性≥99.97%，以上产品服务可用性未达到承诺时，按照服务不可用时间的十倍补偿服务时间，提供原厂盖章承诺函；2、在协助采购人完成互联网医院建设、云平台建设、等保2.0测评、IPv6改造等相关实施过程中，采购人将不予额外支出完成项目所需的其它费用，包括人工、运输、安装、辅材及其它一切与本项目相关的衍生费用。（需要提供承诺函）3、投标人应知晓且明确“整体建设方案满足《GB∕T22239-2019信息安全技术网络安全等级保护基本要求》内第三级要求”，必须协助医院完成基于网络安全等级保护2.0标准的第三方机构测评，综合得分不低于80分；（需要提供承诺函）4、按照“谁建设、运营，谁负责”、“谁管理、使用，谁负责”的原则落实网络安全工作责任，保障安全防护措施与信息化项目同步规划、同步建设、同步使用。投标人应明确对IPv6互联网业务安全管理平台的运维和安全管理责任。5、采购人在租赁过程中收集、产生、存储的数据和文档属于采购人、采购人有权对这些资源访问、利用支配，承建商须严格遵守采购人的相关信息安全规定，不得利用系统维护服务时的便利对采购人数据及其他信息擅自修改或透漏给第三方，未经采购人许可不得访问、修改、披露、转文具、销毁。6、如采购人提前终止某项业务，应在1个月内提前告知投标人，投标人应对停止的业务所涉数据进行安全迁移或可靠的销毁，对账号、地址、域名等及时注销或关闭。（需要提供承诺函）7、发生纠纷时双方应在约定期限内仍能保证采购人数据安全。

1. **服务考核**

1、因服务不到位导致医院出现重大安全问题，导致业务中断（包括但不限于勒索病毒攻击等导致日常业务中断等），应第一时间采取救援措施（包括但不限于支付勒索赎金等），同时根据业务中断时间、影响后果等计赔付额，赔付金额最高可达合同总金额的5倍（需要提供承诺函）；业务虽未中断，但服务响应不及时，发生用户投诉，每次实质性投诉扣款人民币1000元（以院方函告为准），如连续每月三次或以上有责任投诉，采购人可单方面解除服务合同；（需要提供承诺函和应急方案）。

2、投标人应定期组织对云业务、安全、等保、应急等开展业务培训，每年培训不低于2次、应急演练不低于2次。每少一次扣1000元。

1. **资格性要求**

1、符合《中华人民共和国政府采购法》第二十二条的规定，并提供《中华人民共和国政府采购法实施条例》第十七条所要求的材料：

①在中华人民共和国境内注册，具有营业执照、税务登记证、组织机构代码证或企业

“三证合一”只需提供营业执照复印件并加盖公章；

②投标人需提供投标截止日前近半年内缴纳的任意一个月的任意一项税种的凭据，依法免税的投标人，应提供相应的证明文件（复印件加盖公章）；

③近半年任意一个月缴纳社保资金的有效票据凭证（复印件加盖公章）；

④由会计事务所出具的上年度财务审计报告（复印件加盖公章，当年新成立的公司或

上年度财务审计报告还未完审计完成的可提供银行出具的资信证明原件）；

⑤参加政府采购活动前三年内经营活动中没有重大违法记录的书面声明原件（截至开

标日成立不足3年的供应商可提供自成立以来无重大违法记录的书面声明原件）。

2、信用记录：供应商未被列入“信用中国”网站(www.creditchina.gov.cn)记录失信被执行人或重大税收违法案件当事人名单或政府采购严重违法失信行为”记录名单；不处于中国政府采购网(www.ccgp.gov.cn)政府采购严重违法失信行为信息记录”中的禁止参加政府采购活动期间的方可参加本项目的投标。投标截止日当天，由资格审查小组根据以上要求对各供应商信用记录进行查询，有以上行为的视为无效投标。如相关失信记录已失效，供应商需提供相关证明资料。

3、法定代表人授权函原件、法定代表人及被授权人身份证（正、反面复印件）。

4、本项目不接受联合体投标。

**八、符合性要求**

1、所选云服务商需要通过国家互联网信息办公室等开展的“云计算服务安全评估”（需要提供证明文件，需提供云资源的物理位置）

2、报价是否超过招标文件中规定的预算金额或最高限价的。

3、是否按要求提供证明和承诺材料要求签署、盖章。

4、是否含有采购人不能接受的附加条件。

5、是否存在法律、法规和招标文件规定的其他无效情形的。

**九、单项报价**

采购人如业务增加需求可额外采购云服务并配套安全并加入到本项平台统一管理。（需要提供单项报价）

|  |  |  |  |
| --- | --- | --- | --- |
|  | 项目 | 效期 | 单价 |
| 1 | 8核16G/70G系统盘/500G数据盘/正版操作系统+主机安全 | 1年服务 |  |
| 2 | WAF新增1个域名和防护端口 | 1年服务 |  |
| 3 | 新增一个堡垒机资产+账户 | 1年服务 |  |
| 4 | 新增50M带宽&1个公网IP | 1年服务 |  |
| 5 | 新增一个SSL证书 | 1年服务 |  |
| 6 | 其他 | 1年服务 |  |

为保障医院业务连续性，本报价作为今后续约依据。

**十、评分表（综合评分法）**

|  |
| --- |
| 评分表 |
| 内容 | 满分 | 评分标准 | 分值 |
| 价格分 | 10分 | 投标单位价格分采用低价优先法计算，即满足招标文件要求且投标价格最低的投标报价为评标基准价，其价格分为满分。其他投标单位的价格分统一按照下列公式计算：投标报价得分=（评标基准价/投标报价）×10（四舍五入小数点后保留两位数字）评标委员会认为投标人的报价明显低于其他通过符合性审查投标人的报价，有可能影响产品质量或者不能诚信履约的，评标委员会有权要求其在评标现场合理的时间内提供书面说明，必要时提交相关证明材料；投标人如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。 | 10 |
| 技术部分 | 62分 | 招标文件项目需求中设备及产品配置、技术参数、功能等全部符合招标文件项目需求得满分30分。设备技术参数标“▲”项每负偏离一项扣3分，其他指标项负偏离扣1分，扣完为止。 | 30 |
| 投标人所提供安全产品功能齐全、配置合理、质量性能先进程度、运行稳定性和可靠性，安全建设方案考虑周全无单点故障安全隐患。最高得6分。 | 6 |
| 投标人对需求理解深入，对医疗数据安全性充分考虑，整体建设方案能详细描述系统架构、技术路线、安全保障、扩展性强（资源与安全扩展），方案能突出数据安全（云资源位置、安全组件配置等）及系统访问性能（线路带宽、并发数、延时性等）进行分析与保障，最高得8分。  | 8 |
| 1、为保证平台可靠性与安全性，云技术提供厂商应获得CSA-CMMI5证书；2、要求云技术提供厂商具备中国网络安全审查技术与认证中心的信息安全软件开发服务资质（二级及以上）3、要求云计算提供厂商是《信息技术云计算平台即服务部署要求》（GB/T 37739-2019）起草单位之一每符合一项得2分，全部符合得6分，不符合不得分。**（注：1-3项须提供相关证明材料，并加盖厂家公章）** | 6 |
| 投标人提供完整的应急预案，对运营期间可能出现的严重影响系统运行和数据质量的重大问题，提供有效的预防和补救措施。根据投标人的应急预案的合理性、可操作性进行综合打分。投标人提供的应急响应方案规范合理、可操作性强，突发状况的调度安排、应急处理及时、符合本项目实际情况得6分； | 6 |
| 投标人实施方案及培训方案，要求具有专业技术人员负责设备的安装、调试及技术服务，以及开展技术培训的保证措施，提供相关专业技术人员证件资料。包括但不限于项目人员计划、项目组织计划、项目集成计划、项目文档计划、培训目标、培训计划、培训人员等，充分考虑方案内容完整性、科学性、合理性、可行性，最高得6分。 | 6 |
| 综合实力 | 18分 | 1. 投标人具有信息技术服务运行维护ITSS成熟度一级，得3分，二级及以下得2分，没有不得分；
2. 投标人具有信息系统建设和服务能力等级证书，达到CS4及以上的得3分，CS3及以下的得2分，没有不得分；
3. 投标人售后服务能力符合国家标准GB/T27922，具备星级售后服务认证证书（认证范围包括计算机信息系统集成及相关软件开发的售后服务）。五星级认证的得3分；四星级认证的得2分；其他不得分。
4. 投标人具有①ISO14001环境管理体系认证证书②ISO45001职业健康安全管理体系认证证书③ISO9001质量管理体系认证证书④ISO20000-IT服务管理体系认证证书，有一个证书得0.5分，满分2分；

**（注：1-4项须提供相关证书）**1. 项目经理具有信息系统项目管理师、CISP、CCSRP、ITSS-IT服务工程师证书，有一个证书得1分，满分4分；

**（注：5项均须提供证书及投标人近3个月任意一个月为相应人员缴纳社保的证明，人员无社保缴纳证明不得分**） | 15 |
|  |  | 投标人有与本项目类似的成功案例（须提供有效的合同清单及合同复印件，缺一不可），每案例0.5分，最高1分；投标人具有云相关代理商资质（证明材料），得1分；投标人所投产品具备信息系统等级安全保护三级证书的，得1分。 | 3 |
| 售后运维服务 | 10分 | 投标人提供运维服务方案，要点清晰合理、针对性强（包括运维计划、信息上报、管理制度、日常维护、定期巡检和故障维修等具体方案）投标人提供的运维方案科学、合理、针对性强、详实具体，最高得6分。 | 6 |
| 售后服务体系健全：有原厂技术支持团队（具有CISP等相关认证证书）（1分）与针对本项目的专门运维团队（成员具有公有云能力认证资格证书）（1分）。项目中要求的售后服务承诺材料完整（2分） | 4 |

**附件（响应文件格式）**

响

应

文

件

采购项目名称：

供应商名称：

**一、响应函（格式）：**

**响应函**

致扬州大学附属医院：

我方收到贵方关于 的采购文件，经仔细阅读和研究，我方决定参加此次报价。

一、我方愿意按照采购文件的一切要求，提供本项目的报价，报价见《报价一览表》。

二、我方愿意提供贵院在采购文件中要求的文件、资料（具体内容如下）：

1. 响应函（格式见附件）

2. 资格声明（格式见附件）

3. 资格证明文件：

3.1法人或者其他组织的营业执照等证明文件**(复印件加盖供应商公章)**；
3.2 若法定代表人参加询价的，须提供本人身份证复印件**(原件备查)；**若授权代表参加的，须提供《法人授权书》原件和授权代表身份证复印件**（原件备查）**；

3.3 依法缴纳职工社会保障资金的证明材料**(复印件加盖供应商公章)**(税务、银行或社会保险基金管理部门出具的2022年6月-2022年8月近三个月内任意一个月缴纳职工社会保障资金的缴款凭证或缴款证明)；

3.4 供应商2022年6月-2022年8月近三个月内任意一个月依法纳税的缴款凭证**(复印件加盖供应商公章)；**

3.5 与第（1.4）条相对应的纳税申报表或经会计师事务所审计的2021年度财务报告（成立不满一年不需提供）**(复印件加盖供应商公章)**；
 3.6 参加本次政府采购活动前3年内在经营活动中没有重大违法记录的书面声明**(原件）；**

3.7 供应商信用承诺书**(原件)**；
3.8 供应商未被“信用中国”网站（www.creditchina.gov.cn）、“中国政府采购网"网站 (www.ccgp.gov.cn)列入失信被执行人、重大税收违法案件当事人名单、政府采购严重违法失信行为记录名单**（是否被列入失信名单的查询结果将以网页打印的形式加盖供应商公章）**
4.本项目的特定资格要求：

无。

**上述1-4条必须全部提供，如有遗漏，其整个响应文件无效。**

5. 报价一览表

6. 报价明细表及采购需求响应表（**格式见附件**）

7. 如有以下文件自拟并自行添加至响应函中：

（1）要求采购人提供的配合；

（2）其它（供应商认为有必要提供的声明和文件）。

三、我方同意按采购文件中的规定，本响应文件报价的有效期限为报价截止之日起90天。

四、如果我方的响应文件被接受，我方将履行采购文件中规定的每一项要求，按期、按质、按量，完成交货任务。

五、我方认为贵单位有权决定成交者。

六、我方愿意遵守《中华人民共和国政府采购法》，并按《中华人民共和国合同法》和合同条款履行自己的全部责任。

七、我方认可并保证遵守采购文件的所有规定，放弃对采购文件提出质疑的权利。

八、我方愿意按采购文件的规定交纳报价保证金。如我方在报价截止期后撤回报价及成交后拒绝遵守报价承诺或拒绝在规定的时间内与采购人签订合同，则报价保证金将被贵中心没收。

九、如果我方被确定为成交供应商，我方愿意在见证合同时按采购文件的规定交纳履约保证金。且我方如无不可抗力，又未履行采购文件、响应文件和合同条款的，一经查实，我方愿意赔偿由此而造成的一切损失，并同意接受按采购文件的相关要求对我方进行的处理。

十、我方决不提供虚假材料谋取成交、决不采取不正当手段诋毁、排挤其他供应商、决不与采购人、其它供应商等恶意串通、决不向采购人、采购代理机构工作人员和评委进行商业贿赂、决不在采购过程中与采购人进行协商谈判、决不拒绝有关部门监督检查或提供虚假情况，如有违反，无条件接受贵方及相关管理部门的处罚。

供应商（盖章）：

法定代表人(签字或盖章)：

电话： 传真：

通讯地址： 邮编：

**二、资格声明（格式）：**

资格声明

扬州大学附属医院：

 我公司（单位）参加本次 项目活动前三年内，在经营活动中没有重大违法记录，我公司（单位）愿针对本次 项目进行报价，响应文件中所有关于报价资格的文件、证明、陈述均是真实的、准确的。如有虚假，自愿丧失中标资格，一年内退出扬州市政府采购市场。

 供应商（盖章）：

 法定代表人（签字或盖章）：

日期：

1. **营业执照副本：**

**四、法定代表人授权书(格式)**

本授权书声明： （投标人名称）授权 （被授权人的姓名）为我方就 （项目名称）采购活动的合法代理人，以本公司名义全权处理一切与该项目采购有关的事务。

本授权书于\_\_\_\_\_\_年\_\_\_\_月\_\_\_\_日起生效，特此声明。

被授权人签字：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_

联系电话（手机）：

 单位名称：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

 授权单位盖章：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

地址：

日期：

被授权人身份证复印件：

疫情防控承诺书

本人承诺14天内未接触过“新冠肺炎”确诊或疑似病例，未接触过疫情重点地区人员，未与确诊、疑似病例和疫情重点地区人员有聚餐、聚会、大型会议、其他大型活动等密切接触史，如存在隐瞒上述情况，本人依法承担相应法律责任。

承诺人：

年 月 日

**五、报价一览表（格式）：**

采购清单

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 序号 | 内容 | 名称 | 数量 | 1年单价 | 3年单价  | 3年总价 |
| 1 | 互联网应用服务云资源 | 应用服务器（联空） | 3 |  |  |  |
| 日志服务器（联空） | 1 |  |  |  |
| 数据库服务器（联空） | 2 |  |  |  |
| 平台服务器（内外网转换） | 1 |  |  |  |
| 前置服务器（第三方） | 1 |  |  |  |
| 负载均衡 | 2 |  |  |  |
| 2 | 互联网应用云安全资源（包括但不限于） | 堡垒机 | 1 |  |  |  |
| 防火墙 | 1 |  |  |  |
| 数据库审计 | 1 |  |  |  |
| Web网站安全防护 | 1 |  |  |  |
| SSL证书 | 1 |  |  |  |
| 主机安全 | 8 |  |  |  |
| 3 | 线路租用 | 连接院内网络线路 | 1 |  |  |  |
| 4 | 安全服务 | 云资源安全运营服务 | 1 |  |  |  |
| 合计 |  |

采购人如业务增加需求可额外采购云服务并配套安全并加入到本项平台统一管理。（需要提供单项报价）

|  |  |  |  |
| --- | --- | --- | --- |
|  | 项目 | 效期 | 单价 |
| 1 | 8核16G/70G系统盘/500G数据盘/正版操作系统+主机安全 | 1年服务 |  |
| 2 | WAF新增1个域名和防护端口 | 1年服务 |  |
| 3 | 新增一个堡垒机资产+账户 | 1年服务 |  |
| 4 | 新增50M带宽&1个公网IP | 1年服务 |  |
| 5 | 新增一个SSL证书 | 1年服务 |  |
| 6 | 其他 | 1年服务 |  |

为保障医院业务连续性，本报价作为今后续约依据。

法定代表人或者授权代表（签字或盖章）：

供应商全称（盖章）：

 日期： 年 月 日

**六、参加政府采购活动前 3 年内在经营活动中没有重大违法记录的书面声明(参考格式)**

**声 明**

我公司郑重声明：参加本次采购活动前3年内，我公司在经营活动中没有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。

 供应商名称（公章）：

 被授权代表签字：

 日期： 年 月 日

**供应商信用承诺书**

承诺主体名称：

统一社会信用代码：

为维护公平竞争、规范有序的市场秩序，营造诚实守信的信用环境，共同推进社会信用体系建设完善，树立企业诚信守法形象，本企业对\_ \_项目采购活动郑重承诺如下:

一、对提供给注册登记部门、行业管理部门、司法部门、行业组织以及在政府采购活动中提交的所有资料的合法性、真实性、准确性和有效性负责；

二、严格按照国家法律、法规和规章开展采购活动，全面履行应尽的责任和义务，全面做到履约守信，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条件;

三、严格依法开展生产经营活动，主动接受行业监管，自愿接受依法开展的日常检查；违法失信经营后将自愿接受约束和惩戒，并依法承担相应责任；

四、自觉接受行政管理部门、行业组织、社会公众、新闻舆论的监督；

五、自觉做到自我约束、自我管理，不制假售假、商标侵权、虚假宣传、违约毁约、恶意逃债、偷税漏税、垄断和不正当竞争，维护经营者、消费者的合法权益；

六、提出政府采购质疑和投诉坚持依法依规、诚实信用原则，在全国范围12个月内没有三次以上查无实据的政府采购投诉；

七、严格遵守信用信息公示相关规定，向社会公示信用信息；

八、在“信用中国”和“中国政府采购网"网站网站中无违法违规、较重或严重失信记录；

九、如违反承诺，自愿接受管理部门依法给予的行政处罚，同意将违反承诺的行为作为不良记录记入信用档案，依法依规进行信息公示，并承担所产生的一切法律责任和经济损失。

十、本承诺书自签订之日起生效。

 （注：法定代表人或负责人、主体名称发生变更的应当重新做出承诺。）

　　　　　　　　　　  承诺单位（签章）：

　　　　　　　　　 　 法定代表人（负责人）：

　　　　　　　　　 　年    月    日

**服务承诺**

致：扬州大学附属医院

我公司（单位）参加本次 项目做出如下承诺：

SLA服务协议承诺

SLA定义：单云资源实例服务周期总分钟数：按照单云资源实例服务周期内的总天数╳24（小时）╳60（分钟）计算。单云资源实例服务不可用分钟数：在一个服务周期内单云资源实例不可用分钟数之和。

服务可用性计算方式：服务可用性=（单云资源实例服务周期总分钟数-单云资源实例服务不可用分钟数）/单实例服务周期总分钟数×100%。

服务可用性承诺：云主机服务可用性≥99.97%，数据库审计服务可用性≥99.97%，堡垒机服务可用性≥99.97%，日志审计服务可用性≥99.97%，下一代防火墙服务可用性≥99.97%。

赔偿标准：以上产品服务可用性未达到承诺时，按照服务不可用时间的十倍补偿服务时间。

2、在协助采购人完成互联网医院建设、云平台建设、等保2.0测评、IPv6改造等相关实施过程中，采购人将不予额外支出完成项目所需的其它费用，包括人工、运输、安装、辅材及其它一切与本项目相关的衍生费用。

3、公司方知晓且明确“整体建设方案满足《GB∕T22239-2019信息安全技术网络安全等级保护基本要求》内第三级要求”，在协助医院完成基于网络安全等级保护2.0标准的第三方机构测评，综合得分不低于80分；

 4、公司方按照“谁建设、运营，谁负责”、“谁管理、使用，谁负责”的原则落实网络安全工作责任，保障安全防护措施与信息化项目同步规划、同步建设、同步使用。公司方承担IPv6互联网业务安全管理平台的运维和安全管理责任。

5、公司方在提供服务过程中收集、产生、存储的数据和文档属于采购人、采购人有权对这些资源访问、利用支配，公司方严格遵守采购人的相关信息安全规定，不得利用系统维护服务时的便利对采购人数据及其他信息擅自修改或透漏给第三方，未经采购人许可不得访问、修改、披露、转文具、销毁。

6、在终止某项业务前，公司方对所涉数据进行安全迁移或可靠的销毁，对账号、地址、域名等及时注销或关闭。

7、发生纠纷时双方应在约定期限内仍保证相关数据安全。

 承诺单位（签章）：

　　　　　　　　　 　 法定代表人（负责人）：

　　　　　　　　　 　年    月    日

七、安装调试、培训方案

八、其他材料

合同条款及格式

以下为成交后签定本项目合同的通用条款，成交供应商不得提出实质性的修改，关于专用条款将由采购人与成交供应商结合本项目具体情况协商后签订。

项目名称：扬州大学附属医院信息化提升工程一期云资源与云安全租赁项目

编号：

甲方（采购人/买方）：扬州大学附属医院

乙方（供应商/卖方）：

**1、合同标的**

乙方根据甲方需求，提供下列服务： 云服务器资源、云安全资源、云专线、安全服务 。

服务内容等要求详见磋商文件及乙方响应文件。

**2、合同总金额**

2.1 本合同金额为（大写）：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_元人民币（¥\_\_\_\_\_元）。

2.2 本项目合同中总金额是包括为完成磋商文件、项目需求、采购人要求服务内容中的

的所有内容，供应商应充分考虑为完成上述内容所必须的全部服务所需的所有费用。

2.3 在竞争性磋商文件未列明，而乙方认为履行本合同必需的费用也包含在合同总金额中。

2.4 本合同总金额还包含乙方提供的伴随服务/售后服务费用。

**3、组成本合同的有关文件**

3.1乙方应按磋商文件规定的时间向甲方提供服务的有关技术资料。

3.2 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任何合同条文或资料提供给任何其他人。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。

3.3 关于本项目政府采购的磋商文件、磋商响应文件或与本次采购活动方式相适应的文件及有关附件是本合同不可分割的组成部分，这些文件包括但不限于：

 （1）磋商响应文件； （2）磋商报价文件；

 （3）项目组人员表 （4）技术参数、商务条款响应及偏离表；

 （5）服务承诺； （6）成交通知书；

 （7）甲乙双方补充协议； （8）乙方磋商时提供的响应文件。

**4、知识产权保证**

乙方保证甲方在使用、接受本合同服务或其任何一部分时，不受第三方提出侵犯其专利权、版权、商标权和工业设计权等知识产权的起诉。一旦出现侵权，由乙方负全部责任。

**5、产权保证**

乙方保证所交付的服务和服务所涉及的物品所有权无任何抵押、查封等权利瑕疵。

**6、保证金**

6.1 无

**7、转包或分包**

7.1 本合同禁止转包和分包，本合同范围的服务，应由乙方直接提供的，不得转让或分包给他人提供。

**8、服务期**

8.1本项目服务期为三年，即2022年 月 日至2025年 月 日，合同一年一签

8.2本次合同有效期为一年，即2022年 月 日至2023年 月 日；合同有效期内，乙方违反合同规定或达不到甲方考核要求的，甲方有权提前终止合同，由此造成的所有责任和损失由乙方自行承担。

8.3合同期满后，甲方有权视乙方合同执行情况决定是否签署下一年度服务合同。甲方如无异议，双方另行签署下一年度合同。

**9、货款支付**

9.1 本合同项下所有款项均以人民币支付。

9.2 本合同项下的采购资金由甲方支付，付款前乙方向甲方开具发票。

9.3 支付方式：

付款方式： 本合同为后付费方式，本年度服务期满并服务考核合格后凭开具正规发票付款，项目交付使用后每年按实际资源使用量进行支付，不足一年按实际使用月数支付，月单价为（年报价/12）。

**10、税费**

本合同执行中相关的一切税费均由乙方负担。

**11、质量保证及售后服务**

11.1 乙方应按磋商文件规定及响应文件承诺的技术性能、技术要求、质量标准向甲方提供服务；若无特殊说明，则按国家有关部门最新颁布的标准及规范为准。

11.2乙方应保证其提供的服务是全面和规范的，并完全符合磋商及响应文件。如因乙方提供的服务有瑕疵造成甲方损失的，所需费用由乙方承担。

11.3 服务过程中，乙方应对所提供服务出现的质量及安全问题负责处理解决并承担一切费用。

11.4 按照谁建设谁运营谁负责的原则，本次项目安全工作责任由服务提供方负责。项目内信息系统按等级保护（三）级要求，项目内赠送的系统和软件，也需纳入整体项目安全管理。

11.5 项目提供的云服务，需要通过国家信息互联网办公室等开展的“云计算安全评估”。

11.6 整体项目组所有成员需要与医院签订安全承诺和保密协议。停止服务后的系统数据，经医院确认后需要安全销毁；

11.7 服务项目需要定期组织安全监测评估安全风险，对中高风险漏洞、安全防护存在的问题进行修复，采取防范病毒、攻击、入侵等危害行为的防护措施，做好网络、数据库操作日志留存（不低于六个月）。

**12、交付和验收**

12.1 乙方应当在 年 月 日前完成服务事项，竞争性磋商文件有约定的，从其约定。

在交付前，乙方应作出全面检查和对验收文件进行整理，并列出清单，检验的结果交甲方。

12.2 验收标准：按乙方磋商响应文件的承诺。

**13、违约责任**

13.1 甲方无故逾期验收和无故逾期办理款项支付手续的,甲方应按逾期付款金额每日万分之五向乙方支付违约金。

13.2乙方违约，在消除违约情形前，应按本合同项目总额每日万分之五向甲方支付违约金，甲方可以从待付款项中扣除。

13.3乙方因逾期交付服务项目或因其他违约行为，导致甲方解除合同的，乙方应向甲方支付合同总值5%的违约金，如造成甲方损失超过违约金的，超出部分由乙方继续承担赔偿责任。

13.4 乙方所交的服务项目全部或部分品种、型号、规格、技术参数、质量不符合合同规定及磋商文件规定标准的，乙方更换服务但逾期交付的（甲方拒绝接受的除外），按乙方逾期交付处理；乙方拒绝更换的，甲方可选择解除本合同或本合同的一部分，并可追究乙方的其他违约责任。

**14、不可抗力事件处理**

14.1 在合同有效期内，甲乙双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。不可抗力，是指不能预见、不能避免且不能克服的客观情况，例如战争、严重的地震、洪水等，但一方违约或疏忽导致合同不能履行的不属于不可抗力因素。

14.2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。除甲方书面另行要求外，乙方应尽实际可能继续履行合同义务，以及寻求采取合理的方案履行不受不可抗力影响的其他事项。若不可抗力事件延续120天以上，双方应通过友好协商，确定是否继续履行合同。

**15、争议解决**

15.1 因履行本合同引起的或与本合同有关的争议，甲、乙双方应首先通过友好协商解决；如果协商不能解决争议，甲乙双方同意采取下列两种方式的第（1）种方式解决争议。

（1）向甲方所在地有管辖权的人民法院提起诉讼，适用中华人民共和国法律；

（2）向扬州仲裁委员会按其仲裁规则申请仲裁。

15.2 若甲乙双方任何一方都没有选择解除合同的，为避免扩大损失，在诉讼或仲裁期间，双方应继续履行。

**16、合同其它**

16.1 乙方在服务全过程中的生命、财产等安全工作由乙方全权负责，发生任何的安全事故与甲方无关。

16.2 乙方应诚实信用，严格按照磋商文件要求和响应承诺履行合同，不向甲方进行商业贿赂或者提供不正当利益。

16.3合同经双方法定代表人或授权代表签字并加盖单位公章后并经见证方见证盖章后生效。

16.4 本合同未尽事宜，遵照《民法典》有关条文执行。

16.5 本合同正本一式四份，具有同等法律效力，甲方、乙方、见证方及财政监管部门各执一份。

 甲方：扬州大学附属医院 乙方：

 地址： 地址：

 法定代表人或授权代表： 法定代表人或授权代表：

 联系电话： 联系电话：

日期： 2022年 月 日 日期： 2022年 月 日

**扬州大学附属医院医用设备廉洁购销合同**

甲方：扬州大学附属医院

乙方：

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《中华人民共和国民法典》及医用设备购销合同约定购销医用设备项目。

二、甲方应当严格执行医用设备购销合同采购验收、入库制度，对采购医用设备及发票进行查验、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，不得在乙方报销任何应由其个人承担的费用，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，应于3日内向医院纪检监察部门反映情况。

四、甲方工作人员不得要求或者接受乙方为其住房装修、婚丧嫁娶、家属和子女的工作安排以及出国等提供方便。

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用设备的选择权，不得在学术活动中提供旅游、超标准支付食宿费用。

六、乙方不得接受甲方工作人员介绍的家属或者亲友从事与合同相关的业务。

七、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，不得借故到甲方相关领导、部门负责人及相关工作人员的非办公场所访谈并提供任何好处费。

八、乙方如发现甲方工作人员有违反上述协议者，应向甲方举报（甲方接待部门：医院纪检监察室；举报电话：82981199转监察室）。甲方不得找任何借口对乙方进行报复。甲方对举报属实和严格遵守廉洁协议的乙方，在同等条件下优先考虑与乙方继续合作。

九、乙方如违反本合同，一经发现，甲方有权无条件随时终止购销合同，由此导致甲方最终的采购时间延长带来每天的损失按照设备采购款的0.2%由乙方支付给甲方，必要时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，则严格按照《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。

十、甲方任何工作人员围绕上述采购若有违反行风廉洁自律要求的违法、违纪和违规活动自动默认为其个人私下行为，由此导致的一切后果完全由其本人独立承担，与甲方其他人员无关。

十一、本合同作为医用设备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。本合同一式肆份，甲方执壹份，乙方执贰份，甲方纪检监察部门执壹份。

甲方（盖章）：扬州大学附属医院 乙方（盖章）：

法定代表人： 法定代表人：

（或授权签约人）： （或授权签约人）：

甲方相关人员签名： 经办人签名：

2022 年 月 日 2022 年 月 日

**信息安全保密协议**

**甲方**：扬州大学附属医院（扬州市第一人民医院）

**乙方**：（医疗信息化、系统集成、网络服务、维保服务企业）

鉴于乙方受甲方委托承担    项目，该项目将涉及甲方业务系统的系统结构、系统原代码、系统帐号及口令、数据库内容、业务核心数据，项目建设需了解甲方的业务流程、各业务系统相关数据和信息，并获取相关文档资料。为进一步加强医疗卫生信息化党风廉政和行风建设，规范医疗卫生信息化机构操作行为，有效保障数据安全性、信息保密性等行为，营造隐私保密、安全和谐的实施环境，经甲、乙双方协商，现就文档资料、数据和信息使用所涉及的保密信息达成以下协议：

一、保密信息

1.本协议所称“保密信息”是指由本协议甲方以任何形式（包括但不限于：书面，口头，或以样品、范本、计算机程序或其他形式）向本协议乙方披露的任何信息和资料，以及乙方在工作中接触到的一切属于甲方的信息和资料。

2.上述“保密信息”包括但不限于：

医疗领域敏感信息（药品和耗材数量），业务系统的系统结构、系统原代码、系统帐号及口令、数据库内容、业务核心数据及业务流程、各业务系统相关数据和信息内容，病人隐私信息以及其他专有信息等（以下统称“保密信息”）。

3.“保密信息”不包括下列信息：

（1）在生效日之前或之后成为公众所知（非因乙方的过错）；

（2）乙方没有使用保密信息而独立开发的信息；

（3）乙方从第三方合法获取的信息。

二、权利保证

 甲方保证其向乙方披露的专有信息不侵犯任何第三方的知识产权及其它合法权益。

三、保密义务

1、乙方从甲方获得所有保密信息，乙方仅对保密信息具有使用权，而没有所有权、知识产权及解释权。

2、甲方所披露的保密信息只能被乙方用于本项目的实施工作，不得将甲方所披露的保密信息用于其它任何目的。

3、乙方有义务妥善保管保密信息。乙方承诺采取合理的措施以保证保密信息不被泄露，此种措施应至少与甲方对自己的保密信息所采取的措施相当。

4、乙方仅能向有知悉必要的乙方人员披露保密信息。一经发现对保密信息的任何未经授权的披露或乙方及其人员违反本协议时，乙方应立即通知甲方，并采取措施防止进一步未经授权而使用保密信息。

5、未经甲方的事先书面批准，乙方不得直接或间接以任何形式或任何方式把保密信息或其中的任何部分，披露、透露给任何第三方或者公开，乙方保证不向任何第三方披露本协议的存在或本协议的任何内容。

6、**严禁乙方工作人员利用工作便利以任何途径和方式，为甲方统计医师个人及临床科室有关医药产品（药品、耗材等）用量信息以及病人隐私信息，或为第三方统计提供便利。**若工作中发现其他人员有相关违法违纪或泄露相关信息的行为，应立即与甲方或乙方负责人反馈。

7、乙方应当告知要求其参与本项工作之雇员遵守本协议规定，乙方人员向第三方披露保密信息，或依据该等保密信息向第三方做出任何建议，都被视为乙方违反本协议。如有人员离职需要向甲方报备，并除去相应系统权限。

8、乙方参加本项目的所有人员必须与乙方签有正式的保密协议，并且该人员在知晓保密信息前应已充分了解本协议的内容。

9、乙方不得全部或部分复制或仿造保密信息。

10、甲方人员不得要求乙方为其统计医师个人及临床科室有关医药产品用量信息与患者隐私，或要求其以任何方式向第三方透露保密信息或其中的任何部分，如确实有要求请到信息处备案，并两个以上甲方人员签字确认。

四、违约责任

乙方违反本协议任何规定，均视为违约。**一旦违约立即终止所有项目合作，**同时向有关主管部门报告，并严格按照相关规定处理。

1. 保密期限

自甲方第一次向乙方披露任何保密信息之日后起直至该保密信息合法公开时止，乙方不得向任何第三方披露该保密信息。如果所涉及的保密信息依照国家主管机关或相关法律、法规另有规定的，适用其相关规定。任何一方违反本保密协议，违约方应赔偿守约方因此遭受的损失。

六、争议解决

凡因执行本协议所发生的或与本协议有关的一切争议，双方应通过友好协商解决。如果协商不能解决时，可以向协议履行地或有管辖权的法院提起诉讼处理。

七、其他

1、对于本协议条款的修改，只有经双方授权的代表书面签署方可生效并对双方具有约束力。

2、本协议正本一式两份，甲乙双方各执一份，均具同等法律效力。

3、合同生效日期以乙方第一个代表签字日为准。

甲方（签章）： 乙方（签章）：

日期： 日期：

乙方项目组其他成员签字：

**网络安全协议书**

**甲方**：扬州大学附属医院（扬州市第一人民医院）

**乙方**：（医疗信息化、系统集成、网络服务、维保服务企业）

鉴于乙方受甲方委托承担 项目，该项目将涉及甲方业务网络信息安全，项目建设需进入甲方的网络。根据《网络安全法》有关规定，为进一步加强网络安全建设，有效保障医院各类网络安全性、落实等级保护工作，营造绿色健康的网络环境，保证双方的合法利益，经甲、乙双方协商，现就网络安全责任达成以下协议：

一、双方严格遵守《网络安全法》、《全国人民代表大会常务委员会关于维护互联网安全的决定》、《中华人民共和国计算机信息系统安全保护条例》、计算机信息网络国际联网安全保护管理办法》、《互联网安全保护技术措施规定》等法律法规和规章的有关规定，依法从事相关服务。乙方需要实施的服务行为承担法律、行政、民事责任。

二、甲方建立信息安全责任制度，法定代表人为本单位网络与信息安全第一责任人，相关负责人及相关人员依法承担直接责任或其他相应责任。在甲方通知删除违法和有害信息、责令暂时关闭业务或有关系统时，乙方应立即执行。

三、甲方应在项目实施前、项目实施过程中、项目实施后，就网络信息安全相关事项保持与乙方沟通，并根据沟通意见提供相应的软硬件设施。

乙方应建立和完善网络安全技术措施，定期进行安全风险分析与系统漏洞测试，防止病毒传播和被非法控制为网络攻击的跳板，适时对软硬件进行升级，确保系统安全可靠运行。

四、乙方完善信息安全管理制度和技术防范手段，建立健全公共信息内容自动过滤系统和人工值班监控制度，不制作、复制、发布、传播《计算机信息网络国际联网安全保护管理办法》第五条规定的禁止性信息，自觉遵守法律规范，认真履行社会责任。

五、甲方依法保存备份系统网络运行日志和用户使用日志记录不少于60日，在国家有关机关依法查询时乙方应予以提供。

六、甲方依法建立信息安全保密制度和用户信息安全管理制度，乙方在服务过程中应遵守进（驻）场工程师管理有关要求，遵守保密制度，确保用户和病人隐私资料不泄露。

七、甲方实施不良事件上报制度，对所有信息不安全事件进行记录，乙方在服务过程中发现有害信息应及时控制和处理，保留有关原始记录，并在2小时内报告甲方。

八、甲方依法接受相关管理部门的监督管理和检查，主动向公安机关提供案件线索和工作中所需资料，及时报告计算机信息系统中发生的案（事）件，乙方应无条件及时响应。

九、甲方由于发生信息安全事件未及时采取措施造成严重影响的，公安机关将依据相关法律法规规定予以警告、罚款、直至停止联网、停机整顿等处罚，依法追宄甲方责任，如该行为是乙方服务引起，将追究乙方责任。

十、甲方按网络安全法要求实施等级保护制度，乙方按照相应要求无条件配合，相关费用双方协商解决。

十一、本责任书（承诺书）自签定之日起生效。

甲方（签章）： 乙方（签章）：

日期： 日期：

乙方项目组其他成员签字：