## 2026年业务上云运维服务

# 公开招标文件

**采购单位名称：内蒙古自治区中医医院**

**采购代理机构名称：内蒙古招标有限责任公司**

**项目编号：NMGZCS-G-F-260987**

2026年11月

# 目录

第一章 投标邀请

第二章 投标人须知

第三章 招标内容与技术要求

第四章 投标人应当提交的资格、资信证明文件

第五章 评标

第六章 合同与验收

第七章 投标文件格式与要求

# 第一章 投标邀请

内蒙古招标有限责任公司 受 内蒙古自治区中医医院 委托，采用公开招标方式组织采购 2026年业务上云运维服务 。欢迎符合资格条件的投标人参加投标。

## 一.项目概述

1.名称与编号

项目名称： 2026年业务上云运维服务

项目编号： NMGZCS-G-F-260987

采购计划备案号： 内政采计划[2026]41472

2.内容及划分采购包情况

采购包1：2026年业务上云运维服务

采购包预算金额（元）：4,849,000.00

采购包最高限价（元）：4,849,000.00

报价形式：总价

| 序号 | 标的名称 | 数量 | 标的金额（元） | 计量单位 | 所属行业 | 是否核心产品 | 是否允许进口产品 | 是否属于节能产品 | 是否属于环境标志产品 |
|---|---|---|---|---|---|---|---|---|---|
| 1 | 业务上云服务 | 1.000 | 2,842,000.00 | 项 | 软件和信息技术服务业 | 否 | 否 | 否 | 否 |
| 2 | 弱电运维服务 | 1.000 | 867,000.00 | 项 | 软件和信息技术服务业 | 否 | 否 | 否 | 否 |
| 3 | 等级保护测评服务 | 1.000 | 396,700.00 | 项 | 软件和信息技术服务业 | 否 | 否 | 否 | 否 |
| 4 | 国产化服务器操作系统订阅租用服务 | 1.000 | 447,000.00 | 项 | 软件和信息技术服务业 | 否 | 否 | 否 | 否 |
| 5 | 网络和数据安全服务 | 1.000 | 296,300.00 | 项 | 软件和信息技术服务业 | 否 | 否 | 否 | 否 |

3.是否涉及本国产品

采购包1：

| 序号 | 采购品目名称 | 标的名称 | 产品名称 |
|---|---|---|---|
| 不涉及 | | | |

## 二.投标人的资格要求

1.投标人应符合《中华人民共和国政府采购法》第二十二条规定的条件。

2.开标后资格审查时，投标人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，相关信用情况通过“信用中国”网站、中国政府采购网等渠道查询。

3.落实政府采购政策需满足的资格要求：如属于专门面向中小企业采购的项目,提供货物、工程或者服务的供应商应符合享受中小企业扶持政策，并提供《中小企业声明函》。监狱企业、残疾人福利性单位视同小型、微型企业。

4.本项目的特定资格要求：

采购包1：2026年业务上云运维服务

无

## 三.获取招标文件的时间、地点、方式

详见招标公告

其他要求：

无

## 四.招标文件售价

本次招标文件的售价为0元人民币。

## 五.提交投标文件截止时间、开标时间和地点

详见招标公告

## 六.联系方式

采购代理机构名称： 内蒙古招标有限责任公司

地址： 内蒙古呼和浩特市赛罕区腾飞大道众生大厦综合楼16层

邮编： 010020

联系人： 林静

联系电话： 0471-3255283

采购单位名称： 内蒙古自治区中医医院

地址： 内蒙古自治区呼和浩特市新城区健康街11号

邮编： 010000

联系人： 张芳

联系电话： 0471-5323016

# 第二章 投标人须知

## 一.前附表

| 序号 | 条款名称 | 内容及要求 |
| --- | --- | --- |
| 1 | 划分采购包情况 | 共 1 包 |
| 2 | 采购方式 | 公开招标 |
| 3 | 开标方式 | 远程开标 |
| 4 | 评标方式 | 现场网上评标 |
| 5 | 评标方法 | 采购包1：综合评分法 |
| 6 | 获取招标文件时间 | 详见招标公告 |
| 7 | 保证金缴纳截止时间（同投标文件提交截止时间） | 详见招标公告 |
| 8 | 电子投标文件递交 | 加密的电子投标文件1份，电子投标文件在投标截止时间前上传至内蒙古自治区政府采购网--政府采购云平台。技术支持电话：400-0471-010转2键 |
| 9 | 投标文件数量 | （1）加密的电子投标文件1份（需在投标截止时间前上传至“内蒙古自治区政府采购网--政府采购云平台”）<br>（2）若现场无法使用系统进行电子开评标的，投标人须开标现场递交非加密电子版投标文件U盘（或光盘）0份。<br>（3）纸质投标文件（正本）0份；纸质投标文件（副本）0份。 |
| 10 | 中标人确定 | 甲方授权评标委员会（非招标采购，如谈判、磋商、协商、询价小组）按照采购文件规定的方式确定中标（成交）供应商。 |
| 11 | 联合体投标 | 采购包1：不接受 |
| 12 | 采购代理机构代理费用 | 本项目收取代理服务费<br>代理服务费用收取对象：中标/成交供应商<br>代理服务费收费标准：依据内蒙古自治区工程建设协会印发的《内蒙古自治区建设工程招标代理服务收费指导意见》的通知(内工建协(2022)34号)（服务）下浮20%收取 |
| 13 | 投标保证金 | 不收取保证金 |
| 14 | 电子投标文件签字、盖章要求 | 应按照第七章“投标文件格式与要求”，使用单位电子签章（CA）进行签字、加盖公章。<br>说明：若涉及到授权代表签字的可将文件签字页先进行签字、扫描后导入加密电子投标文件。 |
| 15 | 投标客户端 | 投标客户端需要投标人登录“内蒙古自治区政府采购网--政府采购云平台”自行下载。下载地址：https://www.ccgp-neimenggu.gov.cn/gp-auth-center/login?systemRegion=150001&systemRegion=150001 |

| | | |
|---|---|---|
| 16 | 面向中小企业采购 | 采购包1：<br>属于专门面向中小企业采购，预留比例为100%。 |
| 17 | 有效投标人家数 | 采购包1：3家 |
| 18 | 中标供应商数量 | 采购包1：1名 |
| 19 | 中标候选供应商数量 | 采购包1：3名 |
| 20 | 报价形式 | 详见第一章，“内容及划分采购包情况”。 |
| 21 | 现场踏勘 | 采购包1：组织现场踏勘：否 |
| 22 | 兼投不兼中规则 | 本项目可兼投1包，本项目可兼中1包 |
| 23 | 投标有效期 | 从提交投标（响应）文件的截止之日起 90 日历天 |
| 24 | 其他 | 无 |

## 二.投标须知

1.投标方式采用网上投标，流程如下：

投标人应当在内蒙古自治区政府采购云平台申请或注册账号，完善信息后，才可进行网上投标操作，办理流程请登录内蒙古自治区政府采购网（https://www.ccgp-neimenggu.gov.cn）进行查询。

-投标人登录内蒙古自治区政府采购网页面，点击“政府采购云平台”，输入用户名、密码、验证码完成登录后，点击左侧“交易执行—应标—项目应标”，在未参与项目列表中选择要投标的项目，点击项目的“未参与项目”按钮，进入项目投标信息页面，在右侧选择要投标的采购包，填写“联系人姓名”、“联系人手机号”、“联系人邮箱”等信息点击“确认参与”按钮后，获取所投项目招标文件，并按照招标文件的要求制作、上传电子投标文件。

2.投标保证金

2.1投标保证金缴纳（如需缴纳保证金）

本采购项目支持“电子保函”和“虚拟子账户”两种方式收取投标保证金，同时允许投标人按照相关法律法规自主选择以支票、汇票、本票、保函等非现金形式缴纳保证金。

2.1.1投标人选择“电子保函”方式缴纳保证金的，在所投项目下采购包选择电子保函模式，跳转到内蒙古自治区金融服务平台开具电子保函，投标人需要确保在开标之前完成电子保函的开具。

2.1.2投标人选择“虚拟子账户”方式缴纳保证金的，在进行投标信息确认后，应通过“交易执行—应标—项目应标—已参与项目”，选择缴纳银行并获取对应不同采购包的缴纳金额以及虚拟子账号信息，并在开标时间前，缴纳至上述账号中。付款人名称必须为投标单位全称，且与其投标信息一致。

若出现账号缴纳不一致、缴纳金额与投标人须知前附表规定的金额不一致或缴纳时间超过开标时间，将导致保证金缴纳失败。投标人应认真核对账户信息，将投标保证金足额汇入以上账户，并自行承担因汇错投标保证金而产生的一切后果。投标人在转账或电汇的凭证上应按照“项目编号：***、采购包：***的投标保证金”格式注明，以便核对。

2.1.3投标人选择以支票、汇票、本票、保函等非现金形式缴纳保证金的，投标人将相关证明材料原件扫描添加至投标文件中，同时在开标时提供证明材料。

2.1.4缴纳保证金时间以保证金到账时间为准，由于投标保证金到账需要一定时间，请投标人在投标截止前及早缴纳。

2.2投标保证金的退还

投标人在投标截止时间前放弃投标的，自所投采购包结果公告发出后5个工作日内退还，但因投标人自身原因导致无法及时退还的除外。

未中标人投标保证金，自中标通知书发出之日起5个工作日内退还；中标人投标保证金，自政府采购合同签订之日起5个工作日内退还。

2.3有下列情形之一的，投标保证金将不予退还：

（1）中标后，无正当理由放弃中标资格的；

（2）中标后，无正当理由不与采购人签订合同的；

（3）在签订合同时，向采购人提出附加条件的；

（4）不按照招标文件要求提交履约保证金的；

（5）在签订合同时，投标人要求修改、补充和撤销投标文件的实质性内容的；

（6）投标文件中提供虚假材料的；

（7）与采购人、其他投标人或者采购代理机构恶意串通的；

（8）投标人在提交投标文件截止时间后，撤回投标文件的；

（9）法律法规和招标文件规定的其他情形。

3.全流程电子化交易

各投标人应当在内蒙古自治区政府采购云平台开展与本项目有关的政府采购活动。

各投标人应当在响应文件开启时间前上传加密的最终版电子响应文件至“内蒙古自治区政府采购网”，未在响应文件开启时间前上传电子响应文件的，视为自动放弃。投标人因系统问题无法上传电子响应文件时，请在工作时间及时拨打联系电话400-0471-010。

各投标人应当使用数字证书或者政府采购云平台生成的账号密码登录电子交易系统进行系统操作，并对其操作行为和电子签名、电子印章确认的事项承担法律责任。

3.1远程不见面方式（投标人无需到现场）

投标人使用“投标客户端”编制、签章、生成加密投标文件，同时生成“备用标书”，投标人自行留存，涉及“加盖公章”的内容应使用单位电子公章完成。

投标人的法定代表人或其授权代表应当按照本项目招标公告载明的时间等要求参加开标，在开标时间前30分钟，应当提前登录电子交易系统确认联系人姓名与联系电话。

开标时，投标人应当使用CA证书在开始解密后30分钟内完成全部已投标采购包的投标文件在线解密，若出现系统异常情况，工作人员可适当延长解密时长。如在开标过程中出现意外情况导致无法继续进行时，由代理机构会同采购人决定是否允许投标人导入“备用标书”继续开标。本项目采用电子评标，只对开标环节验证通过的电子投标文件进行评审。投标人在参加开标以前自行对使用电脑的网络环境、驱动安装、客户端安装以及CA证书的有效性等进行检测，保证可以正常使用。具体要求请通过“内蒙古自治区政府采购网-政采业务指南”查询相关操作手册。

开标时出现下列情况的，采购人、采购代理机构应当视为投标人不再参与政府采购活动。

（1）投标人未在规定时间内完成电子投标文件在线解密的；

（2）CA证书无法解密投标文件的；

（3）投标人自身原因造成电子投标文件未能解密的。

3.2现场网上方式（投标人需到现场）

投标人使用“投标客户端”编制、签章、生成加密投标文件，同时生成“备用标书”，由投标人自行刻录、存储，涉及“加盖公章”的内容应使用单位电子公章完成。投标人必须保证电子存储设备能够正常读取“备用标书”，电子存储设备（U盘或光盘）表面、外包装上应简要载明项目编号、项目名称、投标单位名称等信息。

投标人的法定代表人或其授权代表应当按照本项目招标公告载明的时间和地点参加开标。开标时，投标人应当使用CA证书完成全部已投标采购包的投标文件在线解密。如在开标过程中出现意外情况导致无法继续进行时，由代理机构会同采购人决定是否允许投标人导入“备用标书”继续进行。本项目采用电子评标，只对开标环节验证通过的电子投标文件进行评审。

开标时出现下列情况的，采购人、采购代理机构应当视为投标人不再参与政府采购活动。

（1）CA证书无法解密投标文件的；

（2）投标人未按招标文件要求提供“备用标书”的；

（3）投标人自身原因造成电子投标文件未能解密的。

4.投标人可以通过“交易执行-应标-项目应标-已参与项目”查看有无本项目信息。

## 三.说明

1.总则

本招标文件依据《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》和《政府采购货物和服务招标投标管理办法》（财政部令第87号）及国家和自治区有关法律、法规、规章制度编制。

投标人应仔细阅读本项目信息公告及招标文件的所有内容（包括澄清或者修改），按照招标文件要求以及格式编制投标文件，并保证其真实性，否则一切后果自负。

本次公开招标项目，是以招标公告的方式邀请非特定的投标人参加投标。

2.适用范围

本招标文件仅适用于本次招标公告中所涉及的项目和内容。

3.相关费用

投标人应自行承担所有与准备、参加投标有关的费用。不论投标结果如何，采购人或采购代理机构均无义务和责任承担相关费用。

4.各参与方

4.1“采购人”是指依法进行政府采购的国家机关、事业单位、团体组织。本招标文件的采购人特指内蒙古自治区中医医院。

4.2“采购代理机构”是指集中采购机构和集中采购机构以外的采购代理机构。本招标文件的采购代理机构特指内蒙古招标有限责任公司。

4.3“投标人”是指向采购人提供货物、工程或者服务的法人、其他组织或者自然人。

4.4“评标委员会”由采购人代表和评审专家组成。

4.5“中标人”是指取得与采购人签订合同资格的投标人。

5.合格的投标人

5.1符合本招标文件规定的资格要求，并按照要求提供相关证明材料。

5.2单位负责人为同一人或者存在直接控股、管理关系的不同投标人，不得参加同一合同项下的政府采购活动。

5.3为采购项目提供整体设计、规范编制或者项目管理、监理、检测等服务的投标人，不得再参加该采购项目的其他采购活动。

6.以联合体形式进行政府采购的，应符合以下规定:

6.1联合体各方应签订联合体协议书，明确联合体牵头人和各方权利义务，并作为投标文件组成部分。

6.2联合体各方均应当具备《中华人民共和国政府采购法》第二十二条规定的条件，并在投标文件中提供联合体各方的相关证明材料。

6.3联合体成员存在不良信用记录的，视同联合体存在不良信用记录。

6.4联合体中有同类资质的投标人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投标人确定资质等级。

6.5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投标人另外组成联合体参加同一合同项下的政府采购活动。

6.6联合体各方应当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。

6.7如要求缴纳保证金，以联合体牵头人名义缴纳，对联合体各方均具有约束力。

7.语言文字以及计量单位

7.1所有文件使用的语言文字为简体中文。专用术语使用外文的，应附有简体中文注释，否则视为无效。

7.2所有计量均采用中华人民共和国法定的计量单位。

7.3所有报价一律使用人民币，货币单位：元。

8.现场踏勘

8.1招标文件规定组织踏勘现场的，采购人或者采购代理机构按招标文件规定的时间、地点组织潜在投标人踏勘项目现场。

8.2投标人自行承担踏勘现场发生的责任、风险和自身费用。

8.3采购人在踏勘现场中介绍的资料和数据等，不构成对招标文件的修改或不作为投标人编制投标文件的依据。

9.其他条款

无论中标与否，投标人递交的投标文件均不予退还。

## 四.招标文件的澄清或者修改

采购人或采购代理机构对已发出的招标文件进行必要的澄清或修改的，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“内蒙古自治区政府采购网”上发布更正公告进行通知；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截止时间，更正公告的内容为招标文件的组成部分，投标人应自行上网查询，采购人或采购代理机构不承担投标人未及时关注相关信息的责任。

## 五.投标文件

1.投标文件的构成

投标文件应按照招标文件第七章“投标文件格式与要求”进行编写，可以增加附页，并作为投标文件的组成部分。

2.投标报价

2.1投标人应按照第三章“招标内容与技术要求”进行报价。投标总价中不得包含招标文件要求以外的内容，否则，在评审时不予核减。

2.2投标报价包括本项目采购需求和投入使用、实施的所有费用，如主件、标准附件、备品备件、施工、服务、专用工具、安装、调试、检验、培训、运输、保险、税款等。

2.3投标报价不得有选择性报价和附加条件的报价。

2.4投标文件报价出现前后不一致的，按下列规定修正：

（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（报价表）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。

修正后的报价投标人应当采用书面形式，并加盖公章，或者由法定代表人或其授权的代表签字确认后产生约束力，但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，投标人不确认的，其投标无效。

2.5投标人应在“投标客户端”对【报价部分】进行填写，“投标客户端”软件将自动根据投标人填写信息生成“开标一览表（报价表）”、“分项报价表”，若在响应文件中出现非系统生成的“开标一览表（报价表）”、“分项报价表”，且与“投标客户端”生成的“开标一览表（报价表）”、“分项报价表”信息内容不一致，以“投标客户端”在线填写报价并生成的内容为准。

3.投标有效期

3.1投标有效期从提交投标文件的截止之日起算。投标文件中承诺的投标有效期应当不少于招标文件中载明的投标有效期。

3.2出现特殊情况需要延长投标有效期的，采购人以书面形式通知所有投标人延长投标有效期。同意延长投标有效期的投标人少于3个的，招标人应当重新招标。投标人同意延长的，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；投标人拒绝延长的，其投标失效，但投标人有权收回其投标保证金。

4.投标文件的递交

投标人应当在投标截止时间前递交投标文件，否则视为自动放弃投标。

5.投标文件的修改和撤回

投标人在投标截止时间前，可以对所递交的投标文件进行补充、修改或者撤回。投标人应当在投标截止时间前上传加密的最终版电子投标文件至“内蒙古自治区政府采购网-政府采购云平台”。

在提交投标截止时间后，投标人不得补充、修改、替代或者撤回其投标文件。

6.样品

采购人、采购代理机构一般不得要求投标人提供样品，仅凭书面方式不能准确描述采购需求或者需要对样品进行主观判断以确认是否满足采购需求等特殊情况除外。

6.1招标文件规定投标人提交样品的，样品属于投标文件的组成部分。样品的生产、运输、安装、保全等一切费用由投标人自理。

6.2开标前，投标人应将样品送达至指定地点，并按要求摆放并做好展示。若需要现场演示的，投标人应提前做好演示准备（包括演示设备）。

6.3采购活动结束后，对于未中标投标人提供的样品，应当及时退还或者经未中标投标人同意后自行处理；对于中标投标人提供的样品，应当按照招标文件的规定进行保管、封存，并作为履约验收的参考。

## 六.开标、评标、中标公告、中标通知书

1.开标

1.1程序

（1）宣布纪律；

（2）宣布相关人员；

（3）投标人对已提交的加密文件进行解密，由采购人或者采购代理机构工作人员宣布投标人名称、投标价格和招标文件规定需要宣布的其他内容（以开标一览表要求为准）；

（4）参加人员对开标结果进行确认；

（5）开标结束。

1.2疑义

投标人代表对开标过程和开标记录有疑义，以及认为采购人、采购代理机构相关工作人员有需要回避情形的，应当场提出询问或者回避申请。采购人、采购代理机构对投标人代表提出的询问或者回避申请应当及时处理。

投标人对远程不见面方式过程和开标记录有疑义，应在“政府采购云平台-远程开标大厅”中提出，采购代理机构应及时查看、回复。

1.3备注说明

1.3.1投标人不足3家的，不得开标。

1.3.2开标时,投标人使用CA证书参与投标文件解密，投标人用于解密的CA证书应为生成、加密、上传投标文件的同一CA证书。

2.资格审查

2.1公开招标采购项目开标结束后，采购人或者采购代理机构应当依法对投标人的资格进行审查，以确定投标人是否具备投标资格。

2.2资格审查中有任意一项未通过的，审查结果为未通过，未通过资格审查的投标人按无效投标处理。

2.3信用记录查询

查询渠道：通过“信用中国”网站(www.creditchina.gov.cn)和“中国政府采购网”（www.ccgp.gov.cn）进行查询；查询截止时点：本项目资格审查时查询;

查询记录：对列入失信被执行人、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、信用报告进行查询;

采购人或采购代理机构应当按照查询渠道、查询时间节点、查询记录内容进行查询，并存档。对信用记录查询结果中显示

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的投标人作无效投标处理。

## 资格审查表

一般资格要求

采购包1：2026年业务上云运维服务

| 序号 | 资格审查要求概况 | 评审点具体描述 |
| --- | --- | --- |
| 1 | 具有独立承担民事责任的能力 | 审查供应商有效的营业执照或事业单位法人证书或执业许可证或自然人的身份证明。 |
| 2 | 具有良好的商业信誉和健全的财务会计制度 | 审查供应商2025年经审计的财务审计报告或近6个月有效的开户银行出具的银行资信证明文件或出具的“具备良好的商业信誉和健全的财务会计制度声明函”（格式自拟）。 |
| 3 | 有依法缴纳税收和社会保障资金的良好记录 | (1)供应商提供投标文件提交截止之日前一年内(至少一个月)的良好缴纳税收的相关凭据(以税务机关提供的纳税凭据或银行入账单为准)或依法缴纳税收承诺函(格式自拟)。(2)供应商提供投标文件提交截止之日前一年内(至少一个月)缴纳社会保险的凭证(以专用收据或社会保险缴纳清单为准)或依法缴纳社会保险承诺函(格式自拟)。注:其他组织和自然人也需要提供缴纳税收的凭据及缴纳社保的凭据或依法缴纳税收及缴纳社保的承诺函(格式自拟)。依法免税或不需要缴纳社会保障资金的投标人，应提供相应文件或承诺函(格式自拟)证明其依法免税或不需要缴纳社会保障资金。 |
| 4 | 具有履行合同所必须的设备和专业技术能力 | 审查供应商出具的“具有履行合同所必需的设备和专业技术能力”声明函(格式自拟)。 |
| 5 | 参加采购活动前3年内，在经营活动中没有重大违法记录 | 审查投标人参加本次投标活动前3年内在经营活动中没有重大违法记录的书面声明。 |
| 6 | 信用记录 | 开标结束后资格审查时，投标人未被列入失信被执行人、税收违法黑名单、政府采购严重违法失信行为记录名单。 |
| 7 | 联合体投标（若有） | 符合关于联合体投标的相关规定。 |

特定资格要求

采购包1：2026年业务上云运维服务

| 资格审查要求概况 | 评审点具体描述 |
| --- | --- |

落实政府采购政策的资格要求

采购包1：

| 资格审查要求概况 | 评审点具体描述 |
| --- | --- |

| | |
|---|---|
| 面向中小企业情况审查 | 提供《中小企业声明函》，残疾人福利性单位提供《残疾人福利性单位声明函》，监狱企业提供由省级以上监狱管理局、戒毒管理局（含新疆生产建设兵团）出具的属于监狱企业的证明文件。（如供应商以联合体形式参加本采购包的，联合体各方均应当符合本采购包专门面向的企业类型；如供应商合同分包的，分包意向协议中分包意向供应商应当符合本采购包专门面向的企业类型。） |

3.评标

详见第五章

4.中标公告

中标人确定后，采购代理机构在内蒙古自治区政府采购网上发布中标结果公告，同时将中标结果以公告形式通知未中标的投标人，中标结果公告期为1个工作日。

5.中标通知书

发布中标结果的同时，中标人可自行登录“内蒙古自治区政府采购网--政府采购云平台”打印中标通知书，中标通知书是合同的组成部分，中标通知书对采购人和中标人具有同等法律效力。

中标通知书发出后，采购人不得违法改变中标结果，中标人无正当理由不得放弃中标。

## 七.询问、质疑与投诉

1.询问

投标人对政府采购活动事项有疑问的，可以向采购人或采购代理机构提出询问，采购人或采购代理机构应当在3个工作日内作出答复，但答复的内容不得涉及商业秘密。投标人提出的询问超出采购人对采购代理机构委托授权范围的，采购代理机构应当告知其向采购人提出。

2.质疑

2.1投标人认为招标文件、采购过程、中标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，以书面形式向采购人、采购代理机构提出质疑。

投标人在法定质疑期内应当一次性提出针对同一采购程序环节的质疑。提出质疑的投标人应当是参与所质疑项目采购活动的投标人。

潜在投标人已依法获取其可质疑的招标文件的，可以对该文件提出质疑。对招标文件提出质疑的，应当在获取招标文件或者招标文件公告期限届满之日起7个工作日内提出。

2.2采购人、采购代理机构应当在收到投标人的书面质疑后7个工作日内作出答复，并以书面形式通知质疑投标人和其他有关投标人，但答复的内容不得涉及商业秘密。

2.3询问或者质疑事项可能影响中标结果的，采购人应当暂停签订合同，已经签订合同的，应当中止履行合同。

2.4投标人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:

（一）投标人的姓名或者名称、地址、邮编、联系人及联系电话；

（二）质疑项目的名称、编号；

（三）具体、明确的质疑事项和与质疑事项相关的请求；

（四）事实依据；

（五）必要的法律依据；

（六）提出质疑的日期。

投标人为自然人的，应当由本人签字；投标人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。

投标人可以委托代理人进行质疑，代理人提出质疑时应当提交投标人签署的授权委托书。其授权委托书应当载明代理人的

姓名或者名称、代理事项、具体权限、期限和相关事项。

2.5投标人提交的质疑函，应按照内蒙古自治区政府采购网中的“质疑函范本”制作。

2.6接收质疑函的方式。为了使提出的质疑事项在规定时间内得到有效答复、处理，质疑可以由法定代表人或授权代表亲自将质疑函递交至采购人或采购代理机构，也可以通过邮寄、快递等方式提交。质疑函以邮寄、快递方式递交的，以邮寄件上的戳记日期、邮政快递件上的戳记日期和非邮政快递件上的签注日期为质疑提起日期。

接收质疑函的联系部门、联系电话、通讯地址（详见第一章 投标邀请）。

3.投诉

3.1质疑人对采购人、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的时间内作出书面答复的，可以在答复期满后15个工作日内向财政部门提起投诉。

投标人投诉的事项不得超出已质疑事项的范围，但基于质疑答复内容提出的投诉事项除外。

3.2投诉人投诉时，应当提交投诉书和必要的证明材料，并按照被投诉采购人、采购代理机构（以下简称被投诉人）和与投诉事项有关的投标人数量提供投诉书的副本。投诉书应当包括下列内容：

（一）投诉人和被投诉人的姓名或者名称、通讯地址、邮编、联系人及联系电话；

（二）质疑和质疑答复情况说明及相关证明材料；

（三）具体、明确的投诉事项和与投诉事项相关的投诉请求；

（四）事实依据；

（五）法律依据；

（六）提起投诉的日期。

投诉人为自然人的，应当由本人签字；投诉人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。

3.3投诉人提交的投诉书，应严格按照内蒙古自治区政府采购网中的“投诉书范本”制作。

# 第三章 招标内容与技术要求

## 一.项目概况

我院信息化业务已连续五年采用云上托管模式运行，实践表明上云模式在资源弹性、业务连续性和运维效率方面优势明显。现行业务上云及相关服务即将到期，需延续采购保障业务不间断；同时，随着医院业务量持续增长、智慧中医医院试点建设和HIS系统整体升级工作的推进，现有云资源在算力规模、容灾备份、安全防护和运维深度等方面已难以满足需求，需同步扩容深化。此外，门诊楼装修改造后全院弱电系统点位与设备规模显著增加，亟需专业维保力量保障稳定运行。

## 二.主要商务要求、技术要求

### 1.主要商务要求

采购包1：2026年业务上云运维服务

| 序号 | 参数性质 | 类型 | 要求 |
| --- | --- | --- | --- |
| 1 | | 标的提供时间 | 合同签订1个月内完成 |
| 2 | | 标的提供地点 | 内蒙古自治区中医医院 |
| 3 | | 合同履约期限 | 服务期自供应商提供的服务达到医院使用要求、可正常投入服务之日起计算，期限为一年。 |
| 4 | | 合同履约地点 | 内蒙古自治区中医医院 |
| 5 | | 验收要求 | 验收要求：1.项目应在规定的时间内完成，达到使用标准，使用科室主任在信息化系统验收单上签字确认，项目经理向信息统计部主任提出项目总体验收申请。<br>2.信息化项目供应商须按照合同约定交付可运行的系统和相关的文档资料，所交付的文档与文件应当包括纸质及电子版式并可供阅读。提供有关本项目的全套技术资料，满足使用人员对系统的安装、使用、维护、应用开发的需要；提供全面技术培训的记录方案，满足使用人员正常使用、日常维护、处理故障，确保所提供的应用系统能正常、安全运行；供应方在项目交付时应提供的管理类文档如下：项目实施计划、项目实施方案、用户培训计划、项目阶段验收报告等。<br>3.项目经理待资料提交完成，通过采购方确认后确定项目验收时间，邀请专业方向覆盖面包括此项目的专家3人、甲方代表、会议记录员组成专家验收小组对项目进行现场验收，专家组通过验收后出《内蒙古自治区中医医院项目验收评审表》，验收小组成员签字后完成项目验收。 |
| 6 | | 合同支付方式 | 1、合同签订后支付合同总金额50%，达到付款条件起60日内，支付合同总金额的50.00%<br>2、服务期结束验收合格支付合同总金额50%，达到付款条件起60日内，支付合同总金额的50.00% |
| 7 | | 履约保证金 | 需要缴纳履约保证金：不缴纳 |

| | | | |
|---|---|---|---|
| 8 | | 其他 | 售后服务要求及其他商务要求：1、投标人必须提供详细的售后服务计划，服务内容、服务方式及响应时间。投标人必须保证在用户出现整个系统不能正常运行或瘫痪的情况时，30分钟内响应，一小时内到达现场或远程解决。<br>2、需要支持电话咨询、网络远程、定期主动巡检，并为用户提供PC端、移动端（微信服务号）的服务平台，供用户提问，对问题进行跟踪。 |
| 9 | | 其他 | 技术履约内容：满足项目采购需求。 |
| 10 | | 其他 | 商务履约内容：所交付的成果满足采购要求、服务期、服务地点、投标有效期、付款方式等满足采购人需求。 |
| 11 | | 其他 | 质量保修范围和保修期：服务期自供应商提供的服务达到医院使用要求、可正常投入服务之日起计算，期限为一年。 |
| 12 | | 其他 | 知识产权归属、处理方式：供应商应保证其提供的成果的均不存在侵犯第三方知识产权的情形。否则，供应商应向采购人承担违约责任及赔偿由此造成的名誉及经济损失。 |
| 13 | | 其他 | 成本补偿、风险分担约定：本项目为总价报价，项目执行过程中相关费用均包含在内，相关市场风险由中标人承担 |
| 14 | | 其他 | 违约责任与解决争议的方法：所有有关本合同或执行本合同所发生的争议，应首先通过甲乙双方友好协商解决，协商不成的，应将争议提交甲方所在地有管辖权的人民法院诉讼解决。 |

**2.技术标准与要求**

采购包1：2026年业务上云运维服务

标的名称：业务上云服务

| 序号 | 参数性质 | 技术参数与性能指标 |
|---|---|---|
| | • | |

| 序号 | 服务名称 | 技术标准 | 数量 | 单位 |
|---|---|---|---|---|
| 1 | 适应医院整体化信息要求 | 详见附件1 | 1 | 项 |
| 2 | 运营商专线要求 | 详见附件2 | 1 | 项 |
| 3 | 人员配备要求 | 详见附件3 | 1 | 项 |
| 4 | 云机房资源租用及安全服务要求 | 详见附件4 | 1 | 项 |
| 5 | 医院网络资源服务（互联网、医院外网官网）等业务云资源服务 | 详见附件5 | 1 | 项 |
| 6 | 网络安全托管服务 | 详见附件6 | 1 | 项 |

1. **附件1：适应医院整体化信息要求**

| 序号 | | 具体技术（参数）要求 | |
|---|---|---|---|
| 1 | √ | 基础设施运维 | 对不同专线接入云资源、链路及相关设备进行运维。 |
| 2 | ▲ | 云上中心建设服务 | 对云上机房设备及环境进行运维（不包含设备及软件更新、设备及软件重新购置等）。对云业务部署的云上数据中心与内蒙古中医医院数据中心进行一体化运维，保证业务能够在云上数据中心稳定持续运行，云上业务系统月度可用率不低于 99.9%（计划内维护时间除外）。 |
| 3 | ▲ | 容灾备份中心建设服务 | 对容灾机房设备及环境进行运维（不包含设备及软件更新、设备及软件重新购置等）。对云业务部署的数据中心与内蒙古中医医院数据中心形成的同城灾备进行运维，保证关键业务能够在中医院现有的数据中心正常接管运行。 |
| 4 | ▲ | 容灾备份要求 | 提供7×24小时容灾备份技术支持和故障维护服务，确保备份的完整性，一旦发生业务、设备、线路、故障或平台故障，及时恢复备业务及平台运行。故障恢复时间不大于180分钟。 |
| 5 | ▲ | 数据安全实施服务 | 上云的核心虚拟机进行秒级别数据保护，且具备根据用户要求恢复虚拟机的数据的服务。通过专线还可以将云上的数据备份到用户本地。并提供技术方案。提供技术方案证明，需具备基于现有环境，检查现有业务的数据安全现状，生成检查报告，并设计、规划、本异地可行的备份方案。 |

| | | | |
|---|---|---|---|
| 6 | √ | 业务资源调配服务 | 采购人具有宿主机控制权限。虚拟机的CPU、内存、硬盘大小等资源可以根据采购人需求调配（36c/448G/296T资源可由实际需求进行自由调配）。调配后对虚拟机业务的影响时间范围为0到5分钟。 |
| 7 | √ | 云兼容性服务 | 要求兼容主流虚拟化厂商（如 VMware、KVM、Hyper-V 及主流国产华为、华三、深信服、天融信等虚拟化平台）。能跨云平移虚拟机 |
| 8 | √ | 云安全及云网络服务 | 中标方能够对虚拟机的操作系统进行维护，包括系统级别的安全、配置和软件包更新。 中标方能够根据采购人需求对网络进行调整，包括进行端口级映射，ACL调整等。可以根据用户需求对资源的配比进行调整，对虚拟机资源调度进行整合等，协助云上应用的部署工作等。 |
| 9 | √ | 技术对接服务 | 能够实现专属云平台与采购人网络中心私有云平台的平滑对接，对接后可以实现跨三层 网络虚拟机迁移而业务不受影响，真正实现自由上云，自由下云，并可以提供详细的技术实现方案。 |
| 10 | √ | 网络安全 | 提供 IPS，IDS，DDOS，WAF 等网络安全设备进行上云虚拟机的必要防护，同网段虚拟机之间需要通过云安全软件进行安全隔离避免虚拟机之间的相互攻击。并提供技术方案。 |

| | | | | | |
|---|---|---|---|---|---|
| | | | 11 | √ | 云资源的运维运营服务 | 针对我院现有在运行全部业务系统进行运维，并与本地机房实现高可用保障。 |
| | | | 12 | √ | 运维成本分析服务 | 实时、动态分析当前资源占用及配比，针对云上资源运行成本进行分析及优化。 |
| | | | 13 | √ | 资产管理服务 | 需提供不少于1次全面的准备及工作调整，提升快速适应资产、威胁及脆弱性动态变化的能力，具备第一时间应急止损的能力。 |
| | | | 14 | √ | 应用系统监 | 针对医院指定的重要业务系统，根据每个应用系统实际部署情况，提供符合每个应用系统情况的资产管理、运维事件、安全事件、拓扑图、技术指标监控、自动化巡检、应用档案、应用探针实施运维运营服务；提供应用系统用户授权管理，提供每个被纳管的业务系统分别进行授权的能力，可以通过用户权限管理为业务部门、外包外协等用户提供多级授权机制，以满足业务部门、外包单位日常工作需要；提供监控一张图看板调研和制作服务，为每一个应用系统单独梳理和实施并展示。一张图中应该包括：软硬件监控指标、软件运行kpi指标、关键业务数据、常态化安全巡检等内容。一张图应该同时制作和提供拓扑图和详细指标看板两种形式供业务部门和相关厂商运维人员使用； |
| | | | 15 | √ | | 监控一张图看板能够提供多种可编排组件来进行看板制作，组件包括图表组件、统计组件、表格组件、测量组件、文本组件、热力图等组件，最后可以通过可视化配置工具配置完成。实施人员能够通过标准的查询语言以自定义方式将数据展示在组件中，通过拖拽，灵活布局组件的方式配置看板，以便用户和维护人员随时通过可视化配置功能进行调整。为保证工期和降低后期成本，不接受通过二次定制开发方式进行指标扩展。 |

| | | | | | |
|---|---|---|---|---|---|
| | | | 16 | √ | 控和看板 | 要求提供不低于50种常用软件探针清单，要求探针可以独立部署。探针需包括：常见操作系统>3种、常见数据库>5种、常见NOSQL>10种、常见消息中间件>5种、常见大数据平台、常见云平台、常见应用服务器、JVM、Docker、K8S、容器云、nvidia gpu等，并且要求提供SNMP、IPMI、RedFish探针，以满足医院要求；提供应用拓扑图绘制服务，绘制好的拓扑图允许用户自行修改，支持将中间件、数据库、网络设备、服务器设备、安全事件、用户体验感知设备、外部接口等涉及应用系统相关的元素通过配置整合到应用拓扑中，并可以为每个元素自定义指标。指标需支持纯文本、进度条，连接线需支持实线、虚线、动画，动画速度可根据线条属性的数值进行动态变化。 |
| | | | 17 | √ | | 提供应用系统日志实时分析服务，在不收集日志的前提下，对分布式应用各个位置的业务日志、错误日志进行实时分析，从日志内的指定事件产生到在监控看板上体现、并形成告警的事件，整个过程应小于60秒；提供应用系统与流程引擎的结合能力，为应用系统提供配置流程服务；提供资产应用系统综合大屏开发服务，包括：接入应用数量、纳管资产数量、巡检设备情况、事件告警情况、应用系统运行情况、24小时动态、应用系统出口流量、用户体验统计。 |
| | | | 18 | √ | 运维和安全事件集成服务 | 提供集中化的事件中心开发集成服务，提供集中处置运维事件和安全事件服务。要求能够集成第三方网管工具、应用监控工具、安全态势感知、漏洞扫描、堡垒机、虚拟化云平台等系统的安全告警、运维事件，以实现事件集成和集中处置。 |
| | | | 19 | √ | | 提供事件等级定义服务，根据管理需要协助医院进行运维事件等级分类管理，并集成来自不同平台的告警事件自动归集到同等级事件中；提供事件超时自动关闭功能，可配置事件超时规则，系统能够根据超时规则自动关闭过期事件，减少运维人员工作量；提供安全和运维事件全生命周期日志，包括事件的产生、规则匹配情况、自动或人工处置记录、事件关闭等全过程信息的审计； |
| | | | 20 | √ | | 提供事件处置规则引擎，根据事件标签定义对事件自动匹配，并可设定规则有效期、消息模板、优先级，同时支持电话外呼、自动派工单；提供事件消息模板自定义功能，包括：信息模板、电话模板，模板中的标题、接收人、内容均需要支持宏定义能力。 |
| | | | 21 | √ | | 提供智能告警规则配置，根据业务需要，进行告警规则合并和抑制；抑制指标的偶发性波动；一个故障原因导致的多设备和系统故障，只报源头；关联性故障，可以只报源头，也可以回溯告警；系统维护期间，可以设置静默时间段，不告警。 |
| | | | 22 | √ | | 提供短信、电话、微信、企业微信、钉钉等多种方式的告警通知能力；需要支持根据事件规则，触发不同类型的流程工单、工单标题需要支持宏定义，可将多个告警标签组合作为工单标题，以便接单人通过工单标题快速了解问题；提供告警事件关联资产、应用的功能，事件能够自动归集到资产和系统档案中，便于业务人员查看和处理。 |

| | | | | | |
|---|---|---|---|---|---|
| | | 23 | √ | CMDB资产梳理服务 | 提供IT资产CMDB数据库梳理服务，能够提供自定义资产大小类别定义，可根据实际情况设置资产的大小类别，提供资产类别关联资产属性模板，以实现资产属性的灵活定义。 |
| | | 24 | √ | | 资产模板需通过可视化的方式进行配置，以满足资产精细化管理，可视化属性设计器需要支持：单行文本、多行文本、日期控件、时间控件、下拉控件、文本描述、表格控件，控件属性需支持：控件默认值、是否必填项、数据格式、验证规则、长度等。 |
| | | 25 | √ | | 资产小类提供状态监测通用规则，通过输入规则，来展示资产的在线情况、存活状态等，监测规则需要支持宏定义；提供资产的新增、删除、编辑、复制、拆分、导入、导出、脱保统计、报废统计、使用年限统计功能；提供基于PN码的产品库，用于资产快速录入，通过输入PN码，快速获取资产详细信息，并可更新PN产品库。 |
| | | 26 | √ | | 提供多维度资产管理视图，可通过商务维度、位置维度、网络维度进行维护管理资产，并提供卡片&列表多种展现形式；提供告警事件、安全风险、资产档案、点巡检、自动巡检等资产数据聚合，在资产视图可以直观的查看围绕资产的相关信息； |
| | | 27 | √ | | 提供资产与安全态势感知、杀毒软件等系统对接，并在资产管理界面展示相关数据；提供资产与流程引擎的结合能力，可以为每一类资产配置多类流程；提供资产展示大屏，包括：仅30天事件趋势、仅30天事件等级、资产分类统计、未关闭事件、目前告警资产、资产等级占比等。 |
| | | 28 | √ | 自动化运维服务 | 针对医院指定的重要业务系统，提供自动化运维实施服务，并提供服务有效期内的无限次自动化运维脚本维护服务。要求运维脚本能够基于系统的脚本模板管理功能，能同时支持ssh、stfp、winrm多种管理协议。支持在一个任务模版种，不同协议的多段脚本混合定义，脚本段执行顺序可定义。提供脚本执行超时定义及采集行数的配置功能。 |
| | | 29 | √ | | 提供模板管理功能，模板支持版本管理，可通过历史版本进行切换版本，并提供发布模板、禁用模板、导入模板、导出模板；为保证自动化脚本运行的安全性，需对脚本模板、自动化作业数据进行加密和数字签名，防伪造、防篡改。要求使用国密算法进行加密和数字签名；提供任务管理模块，通过任务关联模板可进行设备的自动化运维，任务需支持是否对比基线类型，支持自动告警功能，并可设置任务执行周期。 |
| | | 30 | √ | | 提供任务队列查看，可查看当前队列中所有任务，对于未执行的任务，可进行暂停、重启操作，并可追踪历史任务；提供配置文件基线监测、操作系统安全基线自动核查、虚拟机环境准备、上线前自动化检查、数据库备份检查等多种自动化巡检功能，支持通过规则进行按分钟、小时、天等多种周期的监测；提供基线文件的在线对比功能，支持文本对比、时间对比、MD5对比，将文件差异以颜色标注，支持将新配置文件的版本设为基线。 |

| | | | | | |
|---|---|---|---|---|---|
| | | | 31 | √ | 引擎和管理平台需要分离部署，集群化部署，满足高可用和负载均衡需求。提供以应用系统维度查看自动化巡检任务的视图，在应用系统中仅看涉及本系统的所有巡检情况，并直观的显示出所有巡检任务、所有被巡检设备及每个设备的巡检统计情况。 |
| | | | 32 | √ | 人工巡检和标准化作业书管理 提供基于精益管理TPM模型的人工每日巡检、周期点检、精密点检管理服务，并记录巡检结果及处理结果；支持通过流程引擎自定义每日巡检单、可自行配置，并可设置不同审批环节，以适用于不同场景；巡检单支持自动引用系统中的资产数据，并可以将巡检过程中的异常资产数据自动归集至资产病历卡中。 |
| | | | 33 | √ | 周期点检提供：每周一次、每月一次、每年一次年度报告三种点检周期，并可自行设定具体月份，系统根据周期自动形成点检计划，并记录巡检结果及处理结果；周期点检可设置：点检方案、点检路线、被点资产、所属合同，可根据资产类型添加标准化作业书，可按照项目、部门进行逐项检查，并支持一键检查；周期点检、精密点检需按照遵循tpm精益管理八定原则，点检方法需要在5s标准进行设置。 |
| | | | 34 | √ | 等级保护工作管理服务 根据等保安全法，系统需内置提供1-5级等保测评指标，并根据管理要求、技术要求、控制点、分类展示详细指标项，包括：测评标准、测评对象、判定条件、是否高风险项、权重、参考文件；提供应用系统等保自评功能，通过选择应用系统、安全等级，自动拉取测评项，并可以自行增加测评项；支持测评项分配责任人，责任人可通过工作台进入测评，附入佐证材料、流程、文档，并选择测评结论，结论包括：满足、部分满足、不满足、不适用，每项结论均影响测评分数。 |
| | | | 35 | √ | 提供安全等保测评分数计算，通过安全等保测评评分标准及公式，最终得出测评分，便于进行针对性的安全保障；支持以应用系统维度查看等保测评任务，可根据安全建设管理、安全管理人员、安全运维管理、安全管理机构、安全管理制度、安全区域边界、安全计算环境、安全通讯网络、安全物理环境、安全管理中心进行过滤显示。 |
| | | | 36 | √ | 要求使用WEB方式、面向业务人员的可视化、拖拽式、所见即所得的表单设计器，无需安装专用设计工具或插件。支持原有纸质A3/A4／自定义三种格式选择，可手动调整表单的宽度和高度来制作各种样式的文档，100%还原纸张大小，支持高保真还原表格，可生成正式制式标准文档。表单设计器能够使用表单控件快速编辑生成各类简单或复杂的表单，满足不同业务的需要。支持从Word、Excel中复制已经设计好的页面，只需把表单控件放置在对应填表位置上即可。支持HTML代码方式，提供高级用户对表单页面的全面控制支持；表单设计器需同时提供两种不同类型的设计器，方便普通业务人员使用的无格式互联网化的流式表单设计器和模拟纸质样式、打印格式良好的复杂表单设计器。 |

| | | | | | |
|---|---|---|---|---|---|
| | | | 37 | √ | 表单设计器要求提供单行文本、多行文本、附件控件、头像控件、单选框组、多选框组、下拉菜单、超链接控件、签章控件、位置坐标、富文本编辑器等标准控件，支持多维度人员选择控件、多维度组织机构选择控件、编号控件、二维码控件、图片验证码控件、word编辑控件等特殊控件；还需要提供自定义表单业务控件功能，在预定义控件时可以配置数据源，并通过分配业务控件权限的形式达到数据源隔离的目的。 |
| | | | 38 | √ | 要求具备“表单多行”控件，即能够在表单列上动态添加或移除单行文本、多行文本、下拉选择框、日期时间、附件、组织机构等多种类型控件用于加载行列数不固定的动态数据，所有表单列字段均应支持可视化数据源联动；要求控件支持可视化数据源联动与控件联动配置，通过一个控件赋予的值，来联动其他控件； |
| | | | 39 | √ | 流程引擎需支持顺序审批、并行审批、组合审批等多种流程模式；应支持简单条件分支、复杂条件分支、多重分支组合条件分支；提供多人并行审批、并行审批竞争和多人全部处理等流转控制；支持抄送、转发、撤销、附入新流程；支持流程环节指定办理人处理、全部人员审批才可通过及任意一人审批即可通过、退回、取回（允许审批后取回）、接收办理消息、中止、终止、终止重发，流程环节知会人员（审批前知会、审批后知会），流程催办、转办（多级转办）、续办、加签、委托代理等高级业务处理功能；流程引擎支持可选择退回到发起人、退回到上一环节、退回到指定环节三种退回方式。退回到发起人是指发起人退回后可以修改表单，修改附件，重新提交。系统可配置退回后重新提交是按流程固定顺序重新流转，还是可以直接提交到上次退回的环节，直接审批通过；退回到上一环节是指只允许退回到已审批通过的上一环节重新审批或发起；退回到指定环节是指退回到已审批通过的任意环节重新审批或发起；流程引擎需支持环节超时设置功能，启用超时设置后，能够设定流程环节最大办理时限，超时未办理可自动给流程环节办理人发送超时消息提醒。超时提醒可设定消息提醒上限、消息提醒频率、提醒时间范围，以及周末是否免发消息提醒； |
| | | | 40 | √ | 流程节点应支持自动审批，当某节点办理时间超过预设时长后，自动触发办理事件并将本次处理类型标记为超时自动处理。流程节点还可以设置完成权限，拥有完成权限的工作人员可以直接完成该流程，流程将不再进行后续环节，并视为该流程已办结；支持通过可视化配置方式实现表单数据自动采集入库，要求系统能够在流程处理中的任意环节配置采集规则、执行数据采集。支持将表单数据采集到关系型数据库，支持插入式采集、更新式采集（根据关键字更新部分数据字段）或插入更新式采集（存在则更新，不存在则插入），支持将同一个表单数据同时采集到多张表（支持主从表）中； |

| | | | | | |
|---|---|---|---|---|---|
| | | 41 | √ | | 提供数据采集过程的异常监控和处理功能，可全程监控数据采集过程中的异常或警告，并自动添加在异常日志队列中。对日志记录中因采集规则配置不当导致采集失败的可进行单独的人工干预重采、也可将同一批次的异常数据批量执行重采，直至所有数据采集成功；发出警告的表单数据可正常采集入库。管理员可以监管流程使用情况，监测流程事项的发起情况，流程服务的频次，时长，效率等流程汇总信息，出现异常的流程将自动提醒管理员，管理员可直接进行人工介入干预流程。 |
| | | 42 | √ | 自动拨测探针 | 提供和软件系统配套的硬件拨测探针设备，以满足医院内多位置、多协议、多节点，基于专用硬件设备的自动化拨测功能。拨测需支持ICMP\TCP\HTTP协议，并且可以根据业务需要随时扩展。要求提供通过脚本配置，进行模拟登录后对需要认证的业务页面进行拨测的能力；拨测设备要求>=2GB内存、64位双核CPU、双千兆以太网端口，支持远程管理；服务期内，提供只换不修服务。 |
| | | 43 | √ | 自动拨测服务 | 要求针对每个需要拨测的业务系统提供实时统计图，图表内容包括：http连接时间、服务器处理时间、http解析时间、tls连接时间、http传输时间；提供统计百分位图，包括p99、p95、p90、p75、p50，直观的查看用户体验效果，并支持去除超时等异常数据；提供拨测数据包括：平均耗时、最小耗时、最大耗时、标准差等数据，便于观测数据。 |
| | | 44 | √ | | 对分布在医院各处的硬件探针，进行拨测作业自动下发，无需在探针上自行设置，以便随时对拨测作业进行调整和增加。提供在业务系统管理界面中的用户自定义体验感知配置功能，可进行指定业务系统的探测指标、协议类型、数值阈值颜色自定义等设置。 |
| | | 45 | √ | 运维工具软 | 运维工具软件需要同时提供PC、微信、企业微信、医院自用APP等多种方式提供业务访问；负载均衡集群；运维工具软件要求支持基于负载均衡技术的多活集群技术，能够通过简单增加服务器（虚拟机）方式进行业务并发能力的扩展和高可用（高可用，即所有业务节点都可以同时工作，任何一个节点出故障均不会停止服务），要求具备集群令牌、集群缓存功能。 |
| | | 46 | √ | | 运维大数据存储要求：运维工具软件应支持海量运维数据的高速、分布式存储与访问，可采用分布式存储、时序数据库（TSDB）等成熟技术路线，不对底层存储数据库类型作排他性限定，由服务商根据性能与可靠性要求自行选择。 |

| | | | |
|---|---|---|---|
| 47 | √ | 件要求 | 工作条件要求：软件应为开放且符合业界技术标准的系统平台，支持在主流服务器操作系统（如 Windows Server、Linux 各主流发行版、UNIX 等）上部署；支持全文检索技术提供知识库。时序类数据可采用时序数据库（TSDB）或经评估满足性能要求的其他存储方案保存，不对存储技术路线作排他性限定。软件使用的应用服务器应支持主流中间件（如 Tomcat、Weblogic 等及等效产品），具体选型由服务商根据技术架构确定。架构采用 B/S 模式，通过浏览器稳定可靠使用，兼容常用浏览器，访问前后台功能无需安装专用插件（如确需插件，应在投标文件中明确说明并承诺兼容性）。支持多终端访问（包括但不限于 PC、移动 APP、微信、企业微信、钉钉等）；用户数、网元设备数及流程许可应满足本项目业务规模需求，不对合理并发与接入数量作不必要限制。开发能力要求：平台应遵循 OAuth 2.0 标准，为用户及第三方提供基于 RESTful 的开放数据接口（Web Services），并免费提供 SDK 接口与二次开发手册，支持第三方使用主流开发语言进行扩展开发。 |
| 48 | √ | | 安全要求：数据传输应采用 TLS（Transport Layer Security，传输层安全）等成熟加密协议保障安全。其他要求：本次服务涉及的产品和服务，其系统用户数、网元设备数应满足本项目实际业务规模需求，不对合理数量作不必要限制。 |

2. **附件2：运营商专线要求**

| 序号 | | 具体技术（参数）要求 | |
|---|---|---|---|
| 1 | √ | 专线提供服务 | 需提供不同运营商的4条裸光纤，用于院内业务互相负载使用，具体2G1条，1G2条。云部署的物理机房通过4条裸光纤分别以不同路径运营商的物理路由连接医院机房两台核心交换机上4条裸光纤相互负载，在满足医院对网路链路需求的同时，实施网络组件和路径冗余，以支持可用性和负载分配，避免单点故障，提高链路的高可靠性和利用效率。 |

3. **附件3：人员配备要求**

| 序号 | | 具体技术（参数）要求 |
|---|---|---|

| | | | |
|---|---|---|---|
| 1 | √ | 驻场运维人员运维工作要求 | 1.在我院主要领导的具体指导下，承担网络机房运维日常工作安排部署，相关技术方案制定，网络规划及地址分配，设备日常巡检及安全服务巡检和更新维修以及协助院机关各业务处室的部分技术支撑工作；<br>2. 承担互联网规划、局域网网络拓扑结构变动和调整，结合在用信息系统需求，提出网络优化与配置建议。<br>3.承担部分核心交换机、楼层交换机、磁盘阵列、数据备份、防火墙、路由器等常用设备的管理及日常配置。<br>4.积极与运营商沟通，做好管理本单位租用的互联网 IP 地址网段，并掌握地址分配情况。<br>5. 协助采购人梳理本单位外网 IP 地址使用情况。<br>6. 指导驻场运维服务人员的日常管理和调配，每日查看网络的运行使用状况，做到发现问题，适时处置并及时报告。<br>7. 完成采购人交办的与本项目服务范围相符的运维工作任务。<br>8.服务级别：7×24 小时驻场技术服务。提供不低于 4 名工程师驻场技术服务（办公场地由采购人提供），采用轮班方式保障工作日及非工作日均有人员在岗；组建不少于 5 名工程师的技术服务团队，其中包括 1 名项目负责人及一、二线工程师；另提供不少于 2 名三线专家服务团队提供远程服务。 |
| 2 | √ | 服务报告 | 需提供≥1次总结业务运行和服务约定履约情况，提出风险预报、整改方案及未来优化方向。服务次数：≥1次 |
| 3 | √ | 知识库 | 需以用户为单位建立专属知识库、由现场人员进行知识库维护，二线专家团队进行内容审核，下设客户现场各类型常见故障处理流程及方案，故障发生后2小时内极速处理。亦可确保发生人员变动可在3天内快速进入角色。 |
| 4 | √ | 培训服务 | 需提供≥2次向用户提供培训服务，由资深技术专家培训与客户业务相关技术，与维保设备服务方设备运行特性、日常设备维护技巧，常见设备故障处理、关键设备性能。 |
| 5 | √ | 基础架构优化服务 | 需解决不同厂商设备互通时的异构问题以及不同的服务提供商之间的配置差异问题，以提高运维效率，降低配置不规范引发的设备运行风险，减轻运维工作量，提升工作效率，确保业务系统稳定运行，制订统一规划提供储备。 |
| 6 | √ | 数据库性能优化服务 | 需通过数据库自带或三方工具综合分析数据库运行情况。找出性能瓶颈，提供相应的优化服务方案。 |

4. **附件4. 云机房资源租用及安全服务要求**

| 序号 | | 具体技术（参数）要求 | |
|---|---|---|---|
| 1 | ▲ | 整体要求 | 为保障我院数据的安全、稳定运行，供应商提供的所有资源空间及物理承载设备必须为我单位专属使用，不得和其他用户共用或混用。提供的资源空间必须高效稳定的支撑医院内网业务。包括我院现有在运行全部业务系统。 |
| 2 | ▲ | 资源量级要求1 | 云端虚拟化资源1；<br>vCPU 总规模≥2410 核（物理 CPU 单颗≥24 核、主频≥2.2GHz、缓存≥35MB、功耗≤150W，按 vCPU 与主频测算总算力）<br>内存≥4.5TB<br>裸磁盘容量≥不低于383.02TB<br>物理资源；<br>768GB内存最高速率2933MT/s，支持RDIMM或LRDIMM<br>集中存储裸空间36TB |
| 3 | ▲ | 资源量级要求2 | 云端虚拟化资源2；<br>vCPU 总规模≥702 核（国产处理器单颗≥16 核、主频≥2.5GHz、缓存≥64MB、功耗≤260W，按 vCPU 与主频测算总算力）<br>内存≥不低于785GB<br>裸磁盘容量≥不低于32.5TB<br>物理资源；<br>256GB内存最高速率3200MT/s，支持RDIMM或LRDIMM<br>集中存储裸空间10TB |
| 4 | √ | 存储要求 | 平台必须支持直接备份或归档到基于S3接口的对象存储，归档到S3对象存储的数据可支持直接挂载打开读写使用，用于快速恢复数据之用处；支持管理平台节点（包括存储服务器、客户端）的设备运行情况（状态、容量使用情况等）进行统一监控；对于所有操作进行审计，记录配置修改、登录成功/失败、数据恢复等操作；支持对用户密码的安全策略管理，可设置密码的复杂度、有效期等； |

| | | | | | |
|---|---|---|---|---|---|
| | | 5 | √ | | 理论加密流量≥100Mbps,并发用户数≥300，设备吞吐量≥150Mbps,整机并发会话数≥35w；服务设备不少于4个10/100/1000M以太网电口，支持2个USB口和1个RJ45串口，支持单电源；内存≥2G,硬盘容量≥64G SSD； 专业VPN设备，采用标准SSL、TLS 协议，同时支持IPSec VPN、SSLVPN、PPTP VPN、L2TP VPN，非插卡或防火墙带VPN模块设备。同时支持硬件、软件方式交付；支持IPv6的接入；支持IPv6的浏览器访问IPv4的web资源；支持IPv6的windows端访问IPv4的l3vpn资源、TCP资源支持IPv6/IPv4双协议栈； |
| | | 6 | √ | | 支持对基于HTTP、HTTPS、FileShare、DNS、H.323、SMTP、POP3、Telnet、SSH等的所有B/S、C/S应用系统，支持基于TCP、UDP、ICMP等IP层以上的协议的应用；支持PC终端使用包括Windows10、Windows8、Windows7、Windows Vista、Windows xp、Mac OS、Linux等主流操作系统来登录SSLVPN系统，并完整支持该操作系统下的各种IP层以上的B/S和C/S应用；支持主流操作系统的智能手机、PDA、平板电脑（PAD）等移动终端的SSL VPN接入；移动端支持通过PPTP、L2TP VPN方式接入；支持终端使用包括IE6、7、8、10、11或其他IE内核的浏览器，以及最新版本的非IE内核浏览器，最新版登录SSLVPN系统，登录后可完整支持各种IP层以上的B/S和C/S应用；支持国产化终端使用来登录SSLVPN系统，并完整支持该操作系统下的各种IP层以上的B/S和C/S应用；服务设备应支持的密码算法包括：AES、AES192、AES256、DES、3DES、MD5、SHA1、SHA2-256、SHA2-384、SHA2-512、DH、RSA |
| | | 7 | √ | | 可支持个性化登录策略，在一台设备上配置不同的访问域名、IP地址，以及不同的使用界面，实现一台设备为多个不同用户群体服务的的使用效果；支持用户登录界面、服务界面的完全自定义，上传单独的Web页面作为用户登录界面、服务界面；支持智能递推技术，针对多外链的门户网站进行动态嗅探页面内的链接并完成资源自动授权，防止资源漏访；支持Web参数修正，可针对Flash、Java、Applet、或视频播放器对象所引用资源路径进行修正，避免无法播放的问题；服务设备应提供环境检测、自动修复工具，支持对Windows的环境兼容性一键检测能力，以及对检测结果进行一键修复的能力，避免由于用户操作系统环境存在问题影响SSL VPN的使用，减轻运维工作。 |
| | | | | 移动办公 | |

| | | | | | |
|---|---|---|---|---|---|
| | | | 8 | √ | VPN接入服务 | 支持断线重连自动技术，防止用户误操作关闭浏览器导致VPN隧道断开；防止用户在无线网络环境下网络正常切换时VPN隧道断开。服务设备必须支持防中间人攻击，服务设备可在用户登录SSLVPN时智能判断存在中间人攻击行为，断开被攻击的连接，并可提示异常现象；提供HTTPS驱动病毒查杀工具，支持对Windows环境下的针对HTTPS拦截监听的驱动病毒进行扫描查杀，避免因为HTTPS驱动病毒导致无法正常接入和使用SSL VPN；设备内部必须支持自建CA中心，便于数字证书认证平台搭建；支持与基于PKI体系的第三方CA进行结合认证，可根据CA某字段将通过CA认证的用户自动映射到指定用户组，方便进行权限授权配置；支持CRL证书撤销列表； |
| | | | 9 | √ | | 单台VPN设备可扩展同时支持5套以上CA根证书； 支持与第三方认证服务器对接；支持动态令牌认证，支持无需部署令牌认证服务器实现动态令牌认证。 |
| | | | 10 | √ | | 服务设备支持与本方案中终端安全软件联动管理，通过防火墙服务设备界面完成网络中的终端安全软件的安全策略统一管控，实现终端病毒查杀功能。（提供证明截图） |
| | | | 11 | √ | | 支持启用多线路时，自动检测故障线路，并自动踢出故障线路；一旦线路恢复，可在一定时间内自动恢复。支持启用多线路时，自定义用户访问选路策略，包括按上/下行带宽，轮询，按优先级等方式；支持非对称式部署的传输协议优化技术（单边加速），不用在用户终端上安装任何插件和软件，即可提升用户访问应用服务的速度。支持针对不同的web页面进行数据优化，支持动态压缩技术，基于数据流进行压缩，减少不必要的数据传输。基于互联网专线的延伸服务，通过再客户端部署专用网络安全设备与云端系统配合，实现“云+管+端”全场景的网络安全防护，保障客户网络安全和稳定，并提供配套准段SIM卡 |
| | | | 12 | √ | | 支持HTP快速传输协议，大幅优化无线环境（CDMA、GPRS、WIFI、3G）、高丢包、高延等恶劣网络环境下传输速度及效率；支持根据网络境自动选择并切换至最优的传输协议。（需提供服务设备截图证明） |

| | | | | |
|---|---|---|---|---|
| | | 13 | √ | 服务设备要求采用非X86多核架构，配置双交流电源，具备独立的攻击检测引擎与病毒检测引擎；服务设备要求提供3年IPS/AV/ACG特性库升级授权，支持本地、在线两种升级方式；服务设备要求全威胁业务UDP吞吐量≥9Gbps;应用层吞吐量≥4.5Gbps;服务设备要求配置≥14个千兆电接口，≥12千兆光接口，≥4万兆光接口；配置4个千兆多模模块；服务要求支持一体化安全策略，能够基于时间、用户/用户组、应用层协议、五元组、内容安全统一界面进行安全策略配置；服务要求支持策略冗余分析，冲突策略分析以及命中率统计；服务要求支持应用风险调优，通过应用层检测引擎智能地分析安全策略允许通过的流量中存在的潜在风险。 |
| | | 14 | √ | 服务要求攻击特征库数量≥8500、病毒特征库数量≥600W、支持的协议识别数量≥5500、WEB攻击特征库≥3500（提供功能截图） |
| | | 15 | √ | IPS检测到攻击报文或攻击流量后，支持Web重定向、黑名单等响应方式，以实现第一时间隔离有安全威胁的主机；服务设备提供海量预分类的URL地址库，支持根据URL类别实现URL过滤，URL过滤可以基于时间、主机，能够精细到单一IP地址，设备提供海量预分类的URL地址库，支持管理者自定义新的URL地址和URL分类支持URL黑白名单 |
| | | 16 | √ | 提供服务基于用户名（或用户IP地址）实现对用户行为统一分析界面，采用饼状图对访问应用流量、网站访问集中分析展示，包含基于时间轴的访问行为轨迹(应用账号、行为内容等)，关联账号（微信、QQ）等相关用户行为审计内容。（提供功能截图） |
| | | 17 | √ | 服务设备同时支持串接部署模式以及旁路部署模式，支持配置备份和回滚功能，支持软硬件bypass，支持外置bypass主机等方式保障设备掉电网络直通；要求服务设备支持虚拟入侵防御功能：支持虚拟入侵防御的创建、启动、关闭、删除功能；可独立分配CPU/内存等计算资源；可独立管理，独立保存配置；具备独立会话管理、NAT、路由等功能。服务设备支持2台设备堆叠成一台设备使用，实现统一管理，统一配置，所投设备支持高可靠性（包含主备/主主模式）部署。为保证投标服务设备厂商在安全漏洞方面的整体研究水平和及时预防能力。具备网络安全漏洞统一收集验证、预警发布及应急处置体系，进而提高服务设备的安全性。 |
| | | 18 | √ | 服务设备应具有入侵抵御系统，提供有效证书复印件 |
| | | 19 | √ | 服务设备需支持IPV6协议，应具备IPV6证书，提供有效证书复印件 |

| | | | | | |
|---|---|---|---|---|---|
| | | | 20 | √ | 服务设备要求为机架式独立硬件设备，系统硬件为全内置封闭式结构，稳定可靠，加电即可运行，启动过程无须人工干预；服务设备要求为多核架构设计，不允许采用X86架构，采用模块化结构设计；服务设备要求为最大功率≤300W；内置软件Bypass模块，内置两路电口Bypass；在设备流量异常时，可自动切换到Bypass状态，当设备恢复时，可自动切换回工作状态；双电源；服务设备要求为支持10M/100M/1000M自适应电接口数量≥12，支持千兆SFP光接口数量≥12，接口无路由/交换/LAN/WAN等固化区分，均可作为二三层接口使用，支持多桥组部署；服务设备要求为吞吐量≥5Gbps;行为审计&应用控制适用用户规模≥2000人；无线非经支持最大AP数量≥512；服务设备要求支持DDNS客户端以及域名IP绑定功能； |
| | | | 21 | √ | 服务设备要求支持静态路由、策略路由、RIP、OSPF、ISP路由，其中ISP路由支持自定义，并可提供基于应用的策略路由，提供web配置界面截图 |
| | | | 22 | √ | 服务设备要求支持一键化快速审计策略配置。服务设备支持http、邮件、即时通讯、基础协议、娱乐股票、网络应用六个大类维度的用户应用审计。http类审计支持网页访问、网络社区（微博、论坛）、网页搜索、http外发文件、http文件下载、web网盘上传文件、web网盘下载文件等细粒度的审计。 |
| | | | 23 | √ | 服务设备要求支持portal服务器联动portal服务器故障全部用户逃生；服务设备要求支持针对特定域名的APP缓存，只要是该域名传输的APP全部缓存；服务设备支持文件缓存，支持安卓和IOS形式的文件，主动缓存文件形式不限于视频、APP等；服务设备要求支持支持主流厂商的非经对接； |
| | | | 24 | √ | 服务设备支持通过udp 9999同步在线用户、支持radius同步在线用户、支持深澜、城市热点、PPPoe、安美等认证方式的在线用户同步；支持基于http协议获取在线用户同步；服务设备要求支持预定义的入侵攻击特征类，包含最大事件集、常规事件集、应用事件集、攻击事件集。 |
| | | | 25 | √ | 服务设备支持6000+条预定于入侵攻击特征，包括Web服务器防护，包括网页防爬虫、网页防篡改、HTTPS防护、DDoS攻击防护、Web攻击过滤、漏洞防护等，提供配置界面 |

| | | | | | |
|---|---|---|---|---|---|
| | | 26 | √ | 互联网出口防火墙服务2套 | 服务设备规格性能规格：网络层吞吐量≥4G，应用层吞吐量≥2G，并发连接数≥200万，HTTP新建连接数≥6万。服务设备：内存≥4G，硬盘容量≥128G SSD，电源：单电源，网络接口≥8千兆电口+2个千兆光口；服务设备部署方式：支持路由，网桥，虚拟网线，旁路镜像，单臂以及混合部署方式、主备、双机部署模式，实现双机高可用。 |
| | | 27 | ▲ | | 服务设备VPN能力：支持IPSec VPN智能选路功能，根据线路质量和应用实现自动链路切换。提供产品功能截图证明并提供检测报告证明功能有效性 |
| | | 28 | √ | | 服务设备认证方式：支持3种以上的用户认证方式,包含但不限于单点登录、本地账号密码、外部账号密码认证；服务设备双栈协议：支持IPv4/IPv6双栈工作模式，支持IPv6环境的应用控制策略设置，能针对IPv6的IP地址、服务端口、区域、服务/应用、时间等条件进行应用访问规则的设置。 |
| | | 29 | ▲ | | 服务设备入侵防御：支持内置不低于12000种漏洞规则，同时支持在控制台界面通过漏洞ID、漏洞名称、危险等级、漏洞CVE标识、漏洞描述等条件查询漏洞特征信息，支持用户自定义IPS规则。提供产品功能截图证明和第三方检测报告 |
| | | 30 | √ | | 服务设备虚拟防火墙：支持虚拟防火墙功能，支持虚拟防火墙的创建和删除，具备独立的接口、会话管理、应用控制策略、NAT等资源；服务设备访问控制策略：产品支持基于网络区域、网络对象、MAC地址、服务、应用等维度进行访问控制策略设置。 |
| | | 31 | ▲ | | Web应用防护1：支持内置超过4800种WEB应用攻击特征，支持对跨站脚本（XSS）攻击、SQL注入、文件包含攻击、信息泄露攻击、WEBSHELL、网站扫描、网页木马等攻击类型进行防护。提供功能截图第三方检测报告 |
| | | 32 | ▲ | | Web应用防护2：支持服务器漏洞防扫描功能，并对扫描源IP进行日志记录和联动封锁。支持Cookie攻击防护功能，并通过日志记录Cookie被篡改。提供产品功能截图证明和第三方检测报告 |
| | | 33 | √ | | 防病毒： 支持独立的勒索病毒防护模块，非普通防病毒功能，支持对特定的业务进行勒索风险自动化评估，并依据评估结果自动生成防护策略，支持在设备首页独立展示勒索风险板块。提供功能截图并提供关于“勒索病毒”的功能有效性证明 |

| | | | | | |
|---|---|---|---|---|---|
| 1 | | 34 | √ | 互联网区web应用防火墙服务1套 | DDoS防御：支持SYN Flood、ICMP Flood、UDP Flood、DNS Flood、ARP Flood等泛洪类攻击防护，支持IP地址扫描和端口扫描攻击防护；支持ARP欺骗类攻击防护；IP封锁：支持对请求报文头XFF字段检测，并对非法源IP进行日志记录和联动封锁；应用控制：支持应用的识别和控制，应用类型包括游戏、购物、图书百科、工作招聘、P2P下载、聊天工具、旅游出行、股票软件等类型应用进行检测与控制。生命周期管理：支持对安全策略管理和审计功能，记录安全策略变更时间、变更账号、变更类型等内容，提升日常安全策略运维效率。服务设备提供开放API接口（RESTful，Net Conf），可编程管理防火墙，不再仅依赖网管软件。 |
| | | 35 | √ | | 云威胁情报分析： 互联网场景下支持云威胁情报网关技术，实现对威胁流量就近进行实时检测&拦截，实现失陷外联实时阻断，保护资产安全。支持云端未知威胁主动探测技术，实现分钟级内未知威胁情报全网设备下发。提供功能截图或第三方检测报告 |
| | | 36 | √ | | 服务设备要求配置≥8内存，≥1T硬盘，≥2个以太网千兆管理接口，配置≥6以太网千兆电口，≥8个以太网千兆光口，支持≥2个接口扩展槽位；4个千兆多模模块；服务设备要求应用层吞吐量≥1Gbps, HTTP并发连接数≥600000；保护网站站点数量无限制；服务设备支持透明流模式、透明代理模式、反向代理模式、路由牵引模式、镜像检测模式及镜像阻断模式； |
| | | 37 | √ | | 服务设备支持旁路镜像模式下，对检测到的攻击进行旁路阻断；服务设备支持通过BGP方式对流量进行牵引，并在清洗攻击后回注，回注过程支持设置SNAT策略；服务设备支持HTTP协议校验，可根据实际网络状况自定义协议参数合规标准，过滤非法数据；服务设备支持设置扫描陷阱，防止恶意扫描；服务设备支持爬虫防护； |
| | | 38 | √ | | 服务设备支持文件上传、下载过滤；服务设备支持网站批量离线、网站批量恢复、网站一键断网、网站一键恢复操作；服务设备支持攻击态势大屏实时展示，可通过产品自带的实时态势监测模块进行攻击态势地图展示，包含对源地址、源地域、目标服务器、攻击类型、攻击趋势、流量趋势及实时事件的动画统计；态势监测支持对监测范围、防护区域和防护对象的自定义设置； |
| | | 39 | √ | | 要求服务设备提供内网≥6个10/100/1000M RJ45接口，≥2个1000M的SPF光口；外网≥6个10/100/1000M RJ45接口，≥2个1000M的SPF光口；服务设备网络吞吐量：≥700 Mbps；系统整体时延：<1ms； |

| | | | | | |
|---|---|---|---|---|---|
| | | 40 | √ | 网闸服务1套 | 要求服务设备采用2+1架构，专用传输隔离部件完全自主开发且外部无法编程控制；（提供截图）；内外端机为TCP/IP网络协议的终点，阻断TCP/IP协议的直接贯通；内外端机之间采用专用硬件和专用协议进行连接，不可编程。网闸以软硬件结合的方式，有效地隔断内外网络间直接的连接，防止信息无限制交换； |
| | | 41 | √ | | 服务设备只能通过内端机上的管理口对网闸进行配置，外端机上禁止配置管理；提供服务设备安全的文件传输功能，支持FTP、NFS、SAMBA等文件传输协议；提供服务设备对多种主流数据库（SQL、ORACLE、DB2、SYBASE等）数据库系统的安全访问；支持用户查询、修改、添加、删除等操作；服务设备支持全表复制、增量更新、全表更新等； |
| | | 42 | √ | | 服务设备支持各种实例访问；服务设备基于专用客户端与网闸安全连接方式，提供多种主流数据库（SQL、ORACLE、DB2、SYBASE等）的单、双向数据交换；为保证网闸安全性，管理端和审计端需独立与管理口连接使用，禁止使用内端机或外端机上的通讯口对网闸进行配置管理，禁止在外端机上具有管理接口； |
| | | 43 | √ | 互联网区日志审计服务 1套 | 服务设备默认包含主机审计许可证书数量≥50，最大可扩展审计主机许可数≥150，可用存储量≥1TB（RAID1 模式），平均每秒处理日志数（eps）最大性能≥1200。服务设备规格：2U，内存大小：8G，硬盘容量：64GB minisata+1 TB SATA*2，电源：单电源，接口：6千兆电口。支持Syslog、SNMP Trap、数据库、文件、SMB、WMI、Console、日志导入、镜像流量等方式采集日志，审计中心可以支持多个日志采集器 |
| | | 44 | √ | | 支持各类设备的日志采集要求，主要包括：安全设备：国内主流防火墙； 操作系统：Linux、Windows、Windows Server、Unix等操作系统；数据库：Oracle、MySQL、SQLServer等；应用系统： Apache、Tomcat、IIS、Weblogic等；网络设备：主流的路由器、交换机、负载均衡等网络设备等主流网络设备；服务设备支持在安全事件收集引擎上设置过滤条件，可过滤出无关安全事件；支持根据设备类型，按日期展示日志的接入情况，包含不同级别日志数量统计；支持精确的专家模式查询，根据页面的指导提示，通过组合查询表达式完成精确查询 |

| | | | | | |
|---|---|---|---|---|---|
| | | 45 | √ | | 服务设备支持全球地理位置库，支持不同设备相同IP的日志识别；服务设备支持列表的方式展示告警；告警声音设置；告警过滤策略；支持实时监控，滚动显示实时的日志接入信息；服务设备支持关联、审计策略命中后定义告警，响应方式包括：SYSLOG、邮件、自定义命令行。服务设备支持挖掘不同类型、来源于不同设备或系统的日志或安全事件之间可能存在的关联关系，关联的类型包括基于规则和基于统计的。 |
| | | 46 | √ | | 支持根据三权分立的原则和要求进行职、权分离，对系统本身进行分角色定义，如系统管理员只负责完成设备的初始配置，规则配置员只负责审计规则的建立，安全审计员只负责查看相关的审计结果及告警内容；安全管理员只负责完成对系统本身的用户操作日志管理；服务设备支持DNS、DGA、解码错误、解码失败、解码超时的网络会话分类展现；服务设备支持HTTP网页标题、BBS、威胁情报、DGA、搜索关键词的网络会话分类展现；支持TLS会话、数据库会话、邮件会话、FTP会话、Telnet会话，即时通讯会话的展现；服务设备支持定义部门和人员的对应关系，支持定义人员与账号的对应关系 |
| | | 47 | √ | 数据中心防火墙服务2套 | 要求服务设备采用非X86多核架构，具备可插拔冗余电源模块，可插拔冗余风扇模块；要求服务设备吞吐量≥25Gbps，并发连接数≥1000万；提供≥15个SSL VPN并发授权；要求服务设备≥14个千兆电接口；≥8个千兆光接口；≥8个万兆光接口（含模块）；配置冗余电源；支持4个扩展插槽，支持国密板卡扩容；服务设备实现路由模式、透明（网桥）模式、混合模式。实现静态路由、策略路由、RIP、OSPF、BGP等路由协议。 |
| | | 48 | √ | | 服务设备实现一对一、多对一、多对多等多种形式的NAT，实现DNS、FTP、H.323等多种NAT ALG功能。 NAT地址池支持动态探测和可用地址分配；服务设备提供海量预分类的URL地址库，支持根据URL类别实现URL过滤；设备支持管理者自定义新的URL地址和URL分类；服务设备支持联动云端URL地址库进行全面实施核查。服务设备实现安全区域划分，访问控制列表，配置对象及策略，动态包过滤，黑名单，MAC和IP绑定功能，基于MAC的访问控制列表，802.1q VLAN 透传等功能。服务设备支持一体化安全策略，能够基于时间、用户/用户组、应用层协议、五元组、内容安全统一界面进行安全策略配置；支持策略冗余分析，冲突策略分析以及命中率统计。 |

| | | | | | |
|---|---|---|---|---|---|
| | | 49 | ▲ | | 服务设备支持策略风险调优，支持安全策略优化分析，支持策略数冗余及命中分析，支持基于应用风险的策略调优，可根据流量、应用、风险类型等细粒度展示，并给出总体安全评分，便于用户更好的管理安全策略。（提供功能截图） |
| | | 50 | √ | | 服务设备支持不低于6000条以上的应用识别，且提示风险类型及风险级别，便于用户根据实际情况进行上网行为管理。当终端流量流经服务设备时，设备可以分析并提取出终端信息，并支持在终端信息发生变更时向用户发送日志，提示用户。服务设备支持SNMPv1、SNMPv2、SNMPv3、RMON等网络管理协议，并且支持通过网管软件远程进行设备软件升级、配置等。为了保证整个网络的可靠稳定，要求本次提供的安全设备支持A/S，A/A方式部署，支持配置同步和会话同步；提供开放API接口（RESTful，NetConf），可编程管理防火墙，不再仅依赖网管软件。 |
| | | 51 | √ | | 服务设备支持2台设备堆叠成一台设备使用，实现统一管理，统一配置，所投设备支持高可靠性（包含主备/主主模式）部署，提供报告复印件 |
| | | 52 | √ | | 服务设备网络层吞吐量≥3.6Gbps，应用层吞吐量≥450Mbps，带宽性能：300Mb,并发连接数≥150000，每秒新建连接数≥4000，支持用户数≥1500，准入终端数（默认客户端授权数）≥800，包转发率45Kpps；内存大小≥4G，硬盘容量≥1T SATA，电源：单电源，接口≥6千兆电口+2千兆光口SFP。服务设备支持两台及两台以上设备同时做主机的部署模式；服务设备支持部署在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（应用控制、流量控制、内容审计、日志报表等）都支持IPv6； |
| | | 53 | √ | | 服务设备支持发现私接路由（或者共享软件等）共享网络的行为：1.支持自定义配置终端数量和冻结时间。2.支持“仅统计电脑”和“统计所有终端”两种模式。3.支持可选“冻结IP”还是“冻结用户名”。4.支持添加信任列表 5.支持显示以IP或用户名的维度统计一段时间内的趋势图。6.支持例外排除功能：如冻结条件是2. 指定例外条件1台PC，2个终端。当PC或终端数超过例外条件才会被判定为共享。7.支持在数据中心报表中可查询通过共享上网的IP、用户，并能导出报表；（提供产品界面截图） |

| | | | | | |
|---|---|---|---|---|---|
| | | 54 | √ | 内网准入及审计服务 1套 | 服务设备支持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、重定向至制定线路；服务设备支持按剩余带宽、带宽比例、平均分配、前面优先的方式进行多链路负载；支持使用VPN做专线备份；支持链路故障检测；服务设备支持LDAP、Radius、POP3、Proxy等第三方认证；支持ISA\lotus ldap\novel ldap\oracle、sql server、db2、mysql等数据库等第三方认证； |
| | | 55 | √ | | 服务设备支持首页分析显示接入用户人数、终端类型、认证方式；泄密风险、违规访问等行为风险情况；服务设备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；服务设备支持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；服务设备支持图形化查看当前内网IP使用情况，帮助管理员减少人工维护IP表的工作量； |
| | | 56 | √ | | 服务设备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，支持根据IP段、MAC、使用者过滤用户，以便和其他过滤方式一起组合来搜索或获取终端信息；（提供服务设备界面截图） |
| | | 57 | √ | | 服务设备1.对网络接入的终端进行可视化管理，展示终端详细信息、异常状态等 2、支持查看终端类型，以及终端详细信息（厂商，系统，端口等）；3.支持查看终端类型分布；服务设备支持以图表方式显示移动终端接入趋势；服务设备支持短信认证方式，用户输入手机号作为用户名，通过短信猫或短信平台发送验证码； |
| | | 58 | √ | | 服务设备支持802.1x认证，支持对接本地和AD域用户源，支持在旁路模式部署下准入生效；支持未认证前推送认证客户端下载页面，减轻客户端分发工作量；（提供服务设备界面截图） |

| | | | | | |
|---|---|---|---|---|---|
| | | | 59 | √ | 服务设备支持二维码认证，担保人扫描访客的二维码后对其网络访问授权；支持访客填写信息、担保人填写信息、免填写信息三种模式；服务设备支持哑终端通过MAC认证的方式接入网络，必须支持在终端管理列表批量绑定设备IP/MAC快捷放通入网；服务设备支持基于802.1x的外部CA证书认证，同时支持在线证书状态查询（OCSP）；不同用户推送不同认证页面，该认证页面可自定义，编辑内容包括文字、颜色风格、图片，且图片支持轮询播放;服务设备限制某个新用户只能在某个IP段、MAC段范围内登录；认证成功的用户支持页面跳转：1.跳转到用户原本输入的URL地址；2.跳转到管理员指定的URL地址；3.跳转到注销页面; |
| | | | 60 | √ | 支持基于用户组、位置、终端类型、URL类型配置流量管控策略；支持FTP协议上传、下载文件的审计，支持FTP传输客户端的外发附件审计，包括WinSCP、XFftp，FileZilla、SecureFX |
| | | | 61 | √ | 服务设备支持根据标签选择应用，标签分类不低于包含安全风险、高带宽消耗、发送电子邮件、降低工作效率、外发文件泄密风险、主流论坛和微博发帖6大类；支持给每个应用自定义标签；支持根据标签选择一类应用做控制；支持对每一种应用的定义和解释，帮助客户快速定位应用的分类；支持给每一种应用列上图标，易于客户了解应用的特征。（提供服务设备界面截图） |
| | | | 62 | √ | 服务设备支持允许用户登录Webmail收邮件，而禁止发送Webmail邮件的功能；服务设备支持对加密HTTPS、SMTP-SSL、SMTP的邮件进行关键字过滤，支持基于关键字、发件人地址、关键字过滤；支持针对特权用户配置免认证key、免审计key、免控制key；设备必须内置业界知名杀毒引擎；支持检测SYN Flood、ICMP Flood、UDP Flood等泛洪类攻击防护，支持发现异常后告警、封锁主机、推送终端安全软件修复处置；支持防ARP欺骗，支持告警；支持定时广播静态ARP表项；服务设备支持对HTTP、HTTPS、FTP、SMTP、POP3、IMAP协议进行病毒检测和查杀；支持告警通知；支持与云端联动对未知文件进行检测，在设备界面显示云端检测结果。支持识别、阻断、冻结（指定时长）僵尸主机 |
| | | | 63 | √ | 支持查询和导出基于指定时间段/用户/用户组的防共享接入日志、移动终端发现日志、准入日志、登录注销日志等行为日志，支持共享接入、终端类型、接入用户数的排行和趋势分析；支持基于用户和事件类型等维度的上网安全日志统计分析（需提供服务设备功能截图证明） |

| | | | | | |
|---|---|---|---|---|---|
| | | | 64 | √ | 要服务设备求硬件配置≥4G内存，≥2T硬盘，支持2个管理接口，业务接口≥6个以太网千兆电口；≥8个以太网千兆光口，同时支持≥2个接口扩展槽位，支持万兆口扩展；服务设备SQL峰值处理能力≥4万条/秒，日志存储数量≥9亿条，可支持审计4个业务系统，每业务挂载数据库数量不限；服务设备支持对医院的HIS、LIS、EMR、PACS等信息资产全方位监控，对患者就诊信息的篡改、敏感患者就诊信息非法调阅进行追踪告警；内置不同HIS系统的防统方规则库，内置HIS系统不少于9个，且必须包含Caché数据的HIS系统 |
| | | | 65 | √ | 服务设备提供HIS厂商统方规则库，准确识别各种统方操作，同时可根据业务发展自定义规则；支持独立于系统管理员、系统审计员、系统安全员的纪检用户角色，可根据需求配置不同权限的纪检子帐号集，展示纪检用户关心的统方数据；服务设备提供监察人员使用的监察视图，可展示今日、本周以及本月统方事件，同时可根据工号为对象进行二次钻取，展示统方事件分布 |
| | | | 66 | √ | 支持查看返回值信息，可一键查看统方事件中的返回值信息，且返回值内容可自动翻译，敏感字段自动提前展示，帮助使用人员直观看到语句执行结果，辅助判断审计结果（需提供服务配置界面截图） |
| | | | 67 | √ | 服务设备支持医生处方查询分析，可依据时间、帐号、次数进行topN查询分析，结果以表格及分布趋势图展示，并支持三个月的统计对比分析；支持医护人员工号关联展示，通过统方事件中医护人员工号关联展示分析，辅助判断，监察人员可迅速确认统方事件，快速定位相关责任人；服务设备支持统方事件告警，发现统方行为。提供统方事件追踪页面，通过事件关联追踪排查事件，多维度定位事件状态，包括地点追踪、屏幕录像，且屏幕录像与该事件一一对应，支持快捷规则配置；服务设备支持事件告警，发现异常或非法行为。提供事件追踪页面，通过事件关联追踪排查事件，多维度定位事件状态，包括地点追踪、屏幕录像，且屏幕录像与该事件一样对应。支持快捷规则配置；同时，支持对审计数据的多种响应方式，包含过滤、记录、windows消息、邮件、syslog、SNMP、屏幕录像、网关联动等多种事件告警和提示方式，第一时间向负责人发送告警信息 |
| | | | 68 | √ | 支持与物理设备面板一一对应的网卡模拟展示，可根据实际连线情况实时展示网卡当前状态，包含光/电口识别、网卡连通、数据收发、网卡信息等状态，并以水量方式展示网卡当前负载，且支持面板与表格模式切换（需提供服务配置界面截图） |

| | | | |
|---|---|---|---|
| 69 | √ | 财务部业务系统相关计算资源服务配置 | 云主机总规模：提供 4 台隔离专属云主机，整体总 vCPU 算力≥32 核，单台云主机分配 vCPU 不少于 8 核，CPU 主频≥2.9GHz，支持超线程，月结、年终财务批量核算无算力争抢。 |
| 70 | √ | | 内存资源：4 台云主机合计分配物理内存≥288GB，内存为 ECC 纠错 DDR4 规格，数据库节点内存优先分配，支撑财务大报表、成本核算、多并发用户查询，内存资源独占不共享。 |
| 71 | √ | | 存储总容量：配套高速分布式存储总容量≥5.5TB，采用 SSD 混合存储架构，系统盘为 NVMe 高速 SSD，业务数据盘提供高 IO 读写能力，满足财务海量凭证、日志、备份文件存储需求。 |
| 72 | ★ | 开通时间要求 | 合同签订后48小时内开通所有资源服务，保证现有云计算服务和我院所有信息系统业务访问不中断。**(需提供承诺函)** |

5. **附件5：医院网络资源服务（互联网、OA）等业务云资源服务**

| 序号 | | 具体技术（参数）要求 | |
|---|---|---|---|
| 1 | ▲ | 专属计算服务 | 本项目需提供专属硬件资源，可用资源要求如下：VCPU≥124、内存≥320GB、高性能块存储（可用容量）≥7TB，订阅时长12个月。提供承诺函并加盖投标人公章。 |
| 2 | ▲ | | 为了确保本次项目业务的数据安全性，本次采购的云服务需采用硬件独享的模式，云厂商需要提供物理资源独享方案，同时满足本项目资源物理隔离、安全合规等（需提供截图证明，并盖章）； |
| 3 | √ | | 用户可以在专属计算资源的配额内随意创建不同云主机的规格；为了保障本单位业务运行的高可靠性，要求云厂商的云平台在物理资源独享的基础上需提供免费的HA公共备机资源，当本单位的独享服务器宕机后，可自动将公共备机加入到宕机集群中，在备机上恢复云主机的运行状态，并保证故障主机和备机物理介质隔离； |
| 4 | √ | | 为了匹配本单位业务快速发展的需求，要求云厂商提供的云平台需支持云主机在线扩容功能同时满足“热添加”模式，即在业务运行状态下，可以动态增加vcpu和内存的大小；（需提供截图证明，并盖章） |
| 5 | √ | | 为保障数据就近接入性，所提供资源的云节点需要在呼和浩特；云平台允许支持数据重建优先级调整，在故障数据重新恢复时，可由我单位指定优先重建的虚拟机，保证重要的业务优先恢复数据的安全性； |

| | | | |
|---|---|---|---|
| 6 | ▲ | | 承诺云上资源独占、资产可控（独属于客户的专属云服务器）、专属服务器大屏可视、并且在本地就近接入。（提供承诺函并加盖公章） |
| 7 | √ | 互联网带宽服务 | 配置互联网带宽100M，订阅时长12个月 ； |
| 8 | √ | 弹性IP | 为了满足本单位网络与外部网络通信需求，云厂商提供的网络需支持弹性IP功能，云主机、虚拟路由器均能绑定和解绑弹性IP；配置公网IP地址不少于2个，订阅时长12个月； |
| 9 | √ | 网络能力要求 | 为了满足本单位网络安全的需求，服务商需提供VPC内的分布式防火墙，对虚拟机的东西向流量做防护，实现虚拟机之间的微隔离，对数据中心内部流量进行L3-L4层安全防护；<br>为了满足本单位业务进行统一流量审计，服务商提供的网络需满足端口镜像功能，支持VPC网络流量（如：内部云主机）镜像到虚拟安全设备、物理设备；支持跳转连通性探测页面，可以设置探测对象信息，包括网口、对象类型、IP地址，可以点击开始探测按钮查看探测页面信息，可以在网络连通性探测页面查看网络探测是否成功； |
| 10 | ▲ | | 云平台能够通过图形化管理平台的拖放操作完成虚拟网络拓扑的创建和管理，能够通过同一界面中的功能按键，实现虚拟网络连接、开启和关闭等操作；（需提供截图证明，并盖章） |
| 11 | ▲ | | 性能要求：应用层吞吐量≥100M，并发会话数（七层）≥80万，每秒新建会话数≥4万；订阅时长12个月； |
| 12 | √ | | 具备链路故障检测功能，支持通过ARP、DNS、PING协议等方式检测目标主机的可达性，确认接口链路是否有效，并可自定义检测频率；支持基于IP地址、端口、地域、协议、应用等维度配置策略路由策略，支持多种负载均衡算法，包括加权、带宽比例、轮询、线路排序等；产品内置应用特征识别库，支持不少于10000种应用规则，支持对游戏、P2P下载工具、聊天工具、网上银行、视频软件、股票软件、木马控制软件等类型应用进行检测与控制；支持对HTTP、FTP、SMB、SMTP、POP3、IMAP协议进行病毒检测和查杀，支持最大16层的压缩文件查杀； |

| | | | | | |
|---|---|---|---|---|---|
| | | 13 | √ | 下一代防火墙服务资源 | 产品内置IPS检测引擎，支持口令暴力破解、僵尸网络、恶意软件、服务器与终端漏洞攻击等检测和防护，支持超过7000种特征规则；支持僵尸网络检测功能，可基于僵尸网络检测引擎发现主机的异常外联行为，并提供威胁等级和非法外联次数作为举证；产品内置Web应用攻击检测引擎，支持文件包含攻击、抵御注入式攻击（包含SQL注入、系统命令注入）、信息泄露攻击、跨站脚本（XSS）、网站扫描、WEBSHELL后面攻击、跨站请求伪造、目录遍历攻击、WEB整站系统漏洞等应用层攻击行为，支持超过3000种Web服务器漏洞特征规则； |
| | | 14 | ▲ | | 支持对HTTP异常请求协议检测和防护攻击，检测内容包含HTTP请求信息的方法及参数长度等；（需提供产品功能截图证明并盖章） |
| | | 15 | √ | | 具备识别与阻断扫描器发起的服务器恶意扫描行为，可对扫描器地址进行自定义封堵；支持服务漏洞检测功能，基于服务器请求和响应内容识别服务器存在的系统安全漏洞和应用安全漏洞；支持网页恶意链接检测功能，有效识别网页盗链/黑链的行为，避免用户网页资源被滥用；支持Web服务器自动侦测功能，根据Web服务器在线状态、端口使用状态、Web服务器之间的互访关系生成业务资产列表，同时展示内网资产访问的风险等级； |
| | | 16 | ▲ | WEB应用防火墙 | 性能要求：HTTP应用层吞吐量≥100Mbps；HTTP并发连接数≥8W；订阅时长12个月； |
| | | 17 | √ | | 协议合规检测：产品支持对HTTP协议包中各项参数进行合规性控制，通过自定义阈值与参数访问控制相结合的方式，对HTTP数据进行第一层安全控制，从最开始杜绝非法数据包传输。Web攻击防护：产品通过预置Web细粒度的防护特征库，可以有效的对OWASP TOP10攻击行为进行拦截，全面覆盖了WEB应用安全存在的主要威胁，并可根据特定的攻击字段自定义特征，通过匹配的方式对可能出现的攻击执行相应的处理。Web业务控制：产品采用行为分析算法，针对访问行为分析，实现无特征行为的攻击防护，基于访问行为分析可以有效阻断爬虫，黑链，盗链，恶意文件的上传下载等行为。 |

| | | | | | |
|---|---|---|---|---|---|
| | | 18 | √ | | Web敏感信息保护：产品通过中件间信息保护、数据库信息保护、敏感文件保护、代码错误信息保护、隐私信息保护、敏感词防护等诸多敏感信息检测技术，防止敏感信息被泄露。Web业务加固：产品提供深入到具体应用业务内部的专项的加固保护能力，并为每种所支持的应用程序提供专门的检测防御模块，并综合提供多层面的多种检查、控制，从而保护业务的安全性。DDoS攻击防护：产品采用数据采集模型，对经过流量进行分发调配，并配合多核处理架构合理利用系统资源，提升自身处理和清洗能力。 |
| | | 19 | √ | 运维安全管理服务 | 可管理资源数≥10个；系统各模块支持以B/S方式管理，采用https加密方式访问；订阅时长12个月；针对远程终端操作的连接情况进行记录及审计；记录发生时间、发生地址、服务端IP、客户端IP、操作指令、返回信息、操作备注、客户端端口、服务器端口、运维用户帐号、运维用户姓名、审批用户帐号、审批用户姓名、服务器用户名等信息；支持字符协议：SSHv1、SSHv2、TELNET；支持图形协议：RDP、VNC；支持文件传输协议：FTP、SFTP、RDP磁盘映射、RDP剪切板；支持通过协议前置机进行协议扩展，至少支持扩展KVM、Vmware、数据库、http/https、CS应用等； |
| | | 20 | ▲ | | 支持通过动作流配置提供广泛的应用接入支持，无论被接入的资源如何设计登录动作，通过动作流配置都可以实现单点登陆和审计接入（提供截图并盖章）； |
| | | 21 | ▲ | | 用户登陆认证方式支持静态口令认证、手机动态口令认证、Usbkey（数字证书）认证、AD域认证、Radius认证等认证方式；并支持各种认证方式和静态口令组合认证（提供截图并盖章）； |
| | | 22 | √ | | 支持Windows AD域账号与堡垒主机账号周期比对，自动或手动删除或锁定失效的域账号；内置三员角色的同时支持角色灵活自定义，可根据用户实际的管理特性或特殊的安全管理组织架构，划分管理角色的管理范畴；支持RDP安全模式（RDP、NLA、TLS、ANY）设置，以适应RDP-Tcp属性中的所有功能配置，包括加密级别为客户端兼容、低、高、符合FIPS标准等加密级别；支持跨部门的交叉授权操作，部门资源管理员可将本部门资源授权给其他部门用户，实现资源临时/长期跨部门访问； |
| | | 23 | ▲ | | 支持自定义紧急运维流程开启或关闭，紧急运维开启时，运维人员可通过紧急运维流程直接访问目标设备，系统记录为紧急运维工单，审批人员可在事后查看或审批（提供截图并盖章） |

| | | | | | |
|---|---|---|---|---|---|
| | | 24 | √ | | 支持在授权基础上自定义访问审批流程，可设置一级或多级审批人，每级审批可指定通过投票数，需逐级审批通过才可最终发起运维操作；支持定期变更目标设备真实口令，支持自定义口令变更周期和口令强度。口令变更方式至少支持手动指定固定口令、通过密码表生成口令、依照设备挂载的口令策略生成随机口令、依照密码策略生成同一口令等方式；支持密码文件备份功能，密码文件需密文保存，密码包及解密密钥分别发送给不同管理员保存，并使用专用的解密器才可打开； |
| | | 25 | √ | 终端安全服务 | 提供不少于15个服务端授权；订阅时长12个月；支持全网风险展示，包括但不限于未处理的勒索病毒数量、暴力破解数量、僵尸网络、WebShell后门数量、高危漏洞及其各自影响的终端数量；支持终端自动分组管理，新接入的终端可以根据网段自动分配到对应的分组；支持按照扫描网段、扫描方式、扫描协议、扫描端口对终端进行扫描，及时发现尚未纳入管控的终端；支持全网视角的终端资产统一清点，清点信息包括操作系统、应用软件、监听端口和主机账户，其中操作系统、应用软件和监听端口支持从资产和终端两个视角进行统计和展示； |
| | | 26 | ▲ | | 可实时监控文件的状态，在文件读、写、执行或者进入主机时主动进行扫描，支持根据用户性能偏好设置高、中、低3种防护级别（需提供产品截图证明并盖章）； |
| | | 27 | √ | | 支持展示终端检测到的WebShell事件及事件详情，包括：恶意文件名称，威胁等级，受感染的文件，发现时间，检测引擎，文件类型，文件名，文件Hash值，文件大小，文件创建时间；可配置WebShell实时扫描，一旦发现WebShell文件，可自动隔离或仅上报不隔离；基于勒索病毒攻击过程，建立多维度立体防护机制，提供事前入侵防御-事中反加密-事后检测响应的完整防护体系，展示勒索病毒处置情况，对勒索病毒及变种实现专门有效防御（需提供产品截图证明并盖章）；提供内存扫描（挖矿病毒巡检）工具，支持通过内存、进程和启动项来检索病毒相关信息；提供勒索病毒整体防护体系入口，直观展示最近七天勒索病毒防护效果，包括已处置的勒索病毒数量、已阻止的勒索病毒行为次数、已阻止的未知进程操作次数、已阻止的暴力破解攻击次数；（需提供产品截图证明并盖章）；支持按“最近7天”“最近30天”“最近三个月”不同时间维度展示病毒查杀事件爆发趋势和病毒TOP5排行榜，并展示对应的事件数及终端数； |

| | | | | | |
|---|---|---|---|---|---|
| | | 28 | √ | 日志审计服务 | 资产授权数不少于10个；订阅时长12个月；支持主动、被动相结合的数据采集方式，支持通过Agent采集日志数据，支持通过syslog、SNMP Trap、JDBC、WMI、webservice、FTP、文件\文件夹读取、Kafka(截图证明)等多种方式完成日志收集；支持通过正则、分隔符、json、xml的可视方式进行自定义规则解析，支持对解析结果字段的新增、合并、映射；（需提供截图证明并加盖原盖章）；支持对每个日志源设置过滤条件规则，自动过滤无用日志，满足根据实际业务需求减少采集对象发送到核心服务器的安全事件数，减少对网络带宽和数据库存储空间的占用；支持对单个/多个日志源批量转发，支持定时转发，可通过syslog和kafka方式转发到第三方平台，并且支持转发原始日志和已解析日志的两种日志；支持接入TLS加密方式的日志，支持对日志传输状态、最近同步时间进行监控，可统计每个日志源的今日传输量和传输总量； |
| | | 29 | ▲ | | 支持通配符、范围搜索、字段等多种输入方式、搜索框模糊搜索、指定语段进行语法搜索；可根据时间、严重等级等进行组合查询；可根据具体设备、来源/目的所属（可具体到外网、内网资产等）、IP地址、特征ID、URL进行具体条件搜索；支持可设置定时刷新频率，根据刷新时间显示实时接入日志事件；（需提供截图证明，并盖章） |
| | | 30 | √ | | 支持解码小工具，按照不同的解码方式解码成不同的目标内容，编码格式包括base64、Unicode、GBK、HEX、UTF-8等；（需提供截图证明，并盖章）；支持单条事件进行展开，显示事件详细信息和事件原始信息，支持事件详情中任意字段作为查询条件无限制进行二次检索分析；支持网站攻击、漏洞利用、C&C通信、暴力破解、拒绝服务、主机脆弱性、主机异常、恶意软件、账号异常、权限异常、侦查探测等内置关联分析规则，内置关联分析规则数量达到350条以上，支持自定义关联分析规则；日志进行归一化操作后，对日志等级进行映射，根据不同日志源统计不同等级下的日志数量；支持可视化展示，包括数据分布、安全事件趋势图、关联规则告警趋势图、接入设备概况等，可提供设备专项分析场景。如防火墙外部攻击场景分析、VPN账号异常场景分析、Windows服务器主机异常场景分析等，通过设备专项页面对每一台设备安全情况深度专业化分析； |

| | | | | | |
|---|---|---|---|---|---|
| | | 31 | √ | 数据库安全审计服务 | 数据库流量(单向)不小于300Mb/s、数据库无限制；订阅时长12个月；采用B/S管理方式，无需在被审计系统上安装任何代理；无需单独的数据中心，一台设备完成所有工作；提供图形用户界面，以简单、直观的方式完成策略配置、警报查询、攻击响应、集中管理等各种任务；精细化日志秒级查询，通过SQL串模式抽取保障磁盘IO的读写性能；分离式存储SQL语句保障数据审计速度快（需提供截图证明，并盖章）； |
| | | 32 | ▲ | | TB级日志秒级查询、支持指定源IP、时间日期、客户端程序、业务系统、数据库用户、操作类型等精细日志查询、支持操作类型精细化日志查询、支持风险级别排行统计查询、支持数据库条件的统计查询、支持统计趋势查询分析、支持风险级别查询分析、支持通过多SQL语句的统计查询、支持统计分析下钻、支持业务系统元素统计查询（需提供截图证明，并盖章）； |
| | | 33 | √ | | 自定义报表拖拽，通过自定义报表拖拽功能可以随意拖拽用户预期的统计报表，帮助用户提升通过高级选项筛选报表的可读性，更方便达到预期效果；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；支持以风险级别、源IP、业务主机、数据库用户、风险类型为维度的数据库风险排行；数据库威胁分析：可以通过自定义交互分析设置正常访问和异常访问视图、数据库泄密分析、图形化泄密轨迹分析、数据窃取、数据库风险、外发数据人员、受攻击业务系统、风险总次数这几个维度实时监控内网数据威胁态势并且提供交互式分析视图帮助单位快速溯源； |
| | | 34 | ▲ | | 内置大量SQL安全规则，包括如下：导出方式窃取、备份方式窃取、导出可执行程序、备份方式写入恶意代码、系统命令执行、读注册表、写注册表、暴露系统信息、高权存储过程、执行本地代码、常见运维工具使用grant、业务系统使用grant、客户端sp_addrolemember提权、web端sp_addrolemember提权、查询内置敏感表、篡改内置敏感表等；（需提供截图证明，并盖章） |
| | | 35 | ▲ | | 为持续监控公网业务在全国范围内的可用性与连续性，需支持公网场景下的健康检查，可针对业务公网IP地址选择合适探测点发起探测，可选择探测点不可少于5个，且需提供不少于10万次探测免费次数；（需提供产品功能截图，并盖章） |

| | | | | | |
|---|---|---|---|---|---|
| | | 36 | √ | 业务探测服务 | 根据客户业务实际情况，探测任务需支持HTTP/HTTPS、TCP、ICMP等监测协议；支持设置响应头、响应体、状态码、响应时间等断言条件对业务进行实时探测；支持定时拨测，支持设置探测频率，探测频率最高30秒；支持查看拨测失败的响应内容；支持监控信息图表可供查看实时以及历史的拨测趋势图；线上运维管理服务可允许用户登入云上智能运维管理平台，支持用户通过移动端小程序查看业务拨测情况以及用户资源（包括云主机、数据库、服务器、资源池）的监控指标信息；订阅时长12个月； |
| | | 37 | ▲ | 安全基线服务 | 业务系统上线前的安全检查比较复杂，为了避免业务系统上线后由于弱密码、高危端口等脆弱性问题导致业务系统受到攻击，要求云厂商上线前提供弱密码、高危端口的整改闭环服务；（需提供承诺函并加盖公章） |
| | | 38 | √ | | 为保障业务安全，针对用户核心业务弱密码检测规则需包括长度规则、字符规则、字典序、web空密码、账号白名单、密码白名单等，承诺24小时内发现弱密码。检测到弱密码问题后，服务团队需每周一次跟进业务部门闭环弱密码问题；为保障业务安全，针对用户核心业务进行高危端口检测，高危端口类型需包括外网及内网业务，承诺24小时内发现高危端口。检测到高危端口问题后，服务团队需每周一次跟进业务部门闭环高危端口问题；为了避免本单位业务因中勒索病毒遭受重大经济损失，要求云厂商提供的云平台支持勒索病毒防护，通过定时快照服务实现，所有满足条件的虚拟机都按系统定义的频率执行自动快照。发现勒索事件后，专属管家需30分钟内介入，基于存储快照协助恢复数据；（需提供截图证明与承诺函，并盖章）；要求云平台内置自动化安全基线核查工具，支持每周自动扫描并修复不符合等保要求的配置并辅助用户闭环；订阅时长12个月； |

| | | | |
|---|---|---|---|
| 39 | √ | 运维监控服务 | 为了保障本单位业务系统的连续性，提前发现业务存在的风险，要求云厂商提供提供季度巡检报告，从稳定性、性能、容量等方面对云上资源进行巡检，展示运行风险，并提供整改和优化建议；为了满足本单位的在处置疑难问题时的时效性和安全性，要求云厂商支持代维功能，云厂商的运维人员可通过代维协助本单位完成云主机、NFV的配置修改或问题处理，同时本单位可在事后进行录屏下载回看；为满足本单位运维监控的便利性，平台告警和资源状态需支持微信小程序查看：在小程序中能够监控云平台资产和安全设备的告警和资源状态，让我单位对自己的数据中心有“掌控感”。（提供产品功能截图并盖章）；为了保障本单位的服务体验效果，云厂商需为本单位创建专属运维群，且专属运维群支持范围与工单支持范围一致，提供7x24小时技术支持，专属群10分钟内响应。订阅时长12个月。 |
| 40 | ▲ | 云上备份服务 | 为有效防止数据丢失，保障在系统故障或攻击后的业务连续性和数据恢复能力，确保关键数据安全，需提供不少于4600GB的数据高可用备份空间；订阅时长12个月； |
| 41 | √ | | 为了更好的保护用户数据，支持设置定期全量备份，支持用户灵活配置备份策略，备份文件保留时间最高可以达到15年；支持免代理恢复虚拟机整机，也支持对虚拟机文件系统进行解析，以在必要或应急时对虚拟机中的文件、文件夹等进行临时提取； |

6. **附件6：网络安全托管服务需求**

| 序号 | | 具体技术（参数）要求 |
|---|---|---|
| 1 | √ | 服务资产：提供不少于100个业务资产的安全托管服务 |
| 2 | ▲ | 暴露面梳理：投标方应使用安全工具对招标方服务资产开展互联网暴露面探测，以梳理资产面向互联网的开放情况，快速发现违规暴露在互联网中的资产及存在的风险并进行处置，实现对暴露面资产可管可控，降低暴露面资产的风险。投标方应具备互联网暴露面梳理的服务工具，该工具应当支持全资产和精确资产两种模式暴露资产收集模式，收集到的暴露面信息至少包括域名、域名标题、IP地址、开放端口、资产指纹、网站截图、移动端暴露面，并且能采集对应暴露资产的访问截图向招标方举证，及对应暴露资产存在的漏洞。**（提供服务工具具备以上能力的证明材料并盖章）** |

| | | | |
|---|---|---|---|
| 3 | √ | 高危可利用漏洞防护：针对服务范围内资产扫描到的高危可利用漏洞，投标方应当为招标方做好每一个高危可利用漏洞的防护工作，包括但不限于为招标方提供漏洞修复方案和安全设备防护策略，以及帮助招标方配置防护规则，保证招标方不因此出现重大事件和损失；提供服务平台具备高危可利用漏洞防护规则的证明，并且支持对扫描到的高危可利用漏洞能够自动匹配漏洞防护规则。 |
| 4 | √ | 7*24小时威胁鉴定：投标方应当具备云端检测和分析平台，通过采集招标方安全设备和工具的安全告警和安全日志，结合大数据分析、人工智能等技术手段，为招标方提供7*24小时持续不间断的安全威胁分析鉴定，同时在用户界面进行展示；分析研判包括但不限于对脆弱性、异常流量、攻击日志、病毒日志等数据进行采集和实时分析研判，支持将同一资产的多个告警进行聚合分析发现各类安全事件并生成工单，并在告警详情中展示告警的基本信息，涉及的业务信息、攻击趋势、威胁详情、攻击原理、处置建议等内容，并支持根据客户情况提供备注。 |
| 5 | √ | 个性化的检测规则定制：为了保证安全监测的准确率和服务质量，投标方应当支持为招标方自定义配置安全规则，以满足日益复杂的安全趋势所带来的安全监测需求； |
| 6 | √ | 受影响资产排查与加固：安全专家应当结合威胁情报主动排查是否对服务资产造成影响并通知用户，及时协助进行安全加固。（提供一个威胁情报的安全通报工单，工单内容包含威胁情报的基本信息和推送信息以及跟进记录，要求明确说明关联资产信息的排查情况。） |
| 7 | √ | 安全策略检查：投标方安全专家定期对招标方的安全设备的防护策略进行检查，确保安全设备上的安全策略始终处于最优水平，针对威胁能起到最好的防护效果。投标方云端服务平台应当具备丰富的策略检查工具（要求不少于40种策略检查的工具），支持排查安全设备防护策略配置的合理性 |
| 8 | ▲ | 投标方应当为招标方提供7*24小时的安全守护，不论是白天、黑夜、节假日投标方都应该能做到7*24H在线服务，并且在节假日期间应当每日为招标方提供节假日值守快报；投标方应当向招标方承诺，不论白天、黑夜、节假日投标方都能为招标方提供7*24H在线服务，并且在节假日期间能为招标方提供每日的节假日值守快报；**（提供服务具备以上能力的证明材料并盖章）** |
| 9 | √ | 为了降低招标方因网络安全事件造成的损失和影响，投标方应当按照以下服务指标和要求为招标方提供服务：<br>（1）从安全日志上传分析研判到通告给招标方的时间方面，按照国家标准对安全事件的分类分级指南，重大安全事件通告时间小于15分钟，一般事件的通告时间少于30分钟；<br>（2）安全事件经过投标方服务人员的确认后，通告给招标方的各类安全事件的准确率不低于99%（即误报不能超过1%）；<br>（3）投标方应当承诺，服务范围内的所有安全事件的闭环处置比例达到100%。<br>（4）投标方应当满足重大事故应启动应急响应机制，工作时间15分钟之内云端专家进行响应，非工作时间30分钟之内云端专家进行响应。 |

| | | | |
|---|---|---|---|
| 10 | √ | 服务成果可视化：投标方需为招标方提供的服务成果展示门户（或用户Portal），需要提供安全托管服务相关信息的详细展示和呈现，分别为安全运营概览、事件&威胁概况、脆弱性概况、运营交付物报告、服务SLA，并支持全屏投放展示。 |
| 11 | √ | 服务质量监控：投标方需为招标方提供的服务成果展示门户（或用户Portal）应具备服务质量可视化展示，投标方能通过可视化的数据，清晰的了解安全专家的服务水平，至少包括平均研判时间、平均遏制时间MTTC、平均闭环时间MTTR、事件闭环率，以验证投标方所承诺的服务指标（或称为服务SLA）。提供服务成果展示门户中服务质量监控相关的截图证明； |
| 12 | √ | 服务交付物管理：投标方需为招标方提供的服务成果展示门户（或用户Portal），可以直观的管理服务过程中生产的服务报告和交付物，包括但不限于《项目启动会PPT》、《首次安全风险分析报告》、《威胁情报》、《安全运营周报》、《安全运营月报》、《安全运营半年度报告》、《年度总结汇报》等。提供服务成果展示门户中支持下载和管理上述交付物； |
| 13 | ▲ | 服务过程透明化可视化：投标方需为招标方提供移动端服务过程展示门户（移动端Portal），通过清晰可视化的风险消减图和漏洞消减图，让招标方清晰了解云端安全托管服务的风险消减机制，直观实时了解当前风险闭环情况。提供移动端服务过程展示门户中支持展示风险消减图和漏洞消减图。**（提供服务具备以上能力的证明材料并盖章）** |
| 14 | √ | 投标方需为招标方提供移动端服务过程展示门户（移动端Portal），支持直观地查阅服务推送的各种安全事件/威胁的详细专家审核研判过程，需包含安全事件详细的基本信息、定性结论和数据包分析等内容。 |
| 15 | √ | 投标方需为招标方提供移动端服务成果展示门户（移动端Portal），支持直观地管理服务过程中安全运营结果，以“资产、威胁、漏洞、事件四大抓手”为维度，呈现服务后业务实时的安全情况和运营结果。 |
| 16 | √ | 投标方云端服务平台应当做好严格的安全防护，并严格按照《信息安全技术—网络安全等级保护基本要求》完成等级保护测评工作，服务平台至少通过等级保护三级测评；投标方应当提供云端服务平台等级保护三级测评通过证明，提供报告首页、基本信息表、等级测评结论首页，以上内容中必须明确指出该平台用于为用户提供7*24小时的安全托管服务； |
| 17 | ▲ | 为了保障服务效率和质量，投标方的云端服务平台应当具备一套完善的流程编排引擎，能够为客户灵活编排、定义服务流程，并且定义服务的SLA，将服务过程中的各个关键环节按照一定的顺序和规则进行组织和安排，以达到高效、优质的服务目标；投标方应当提供云端服务平台具备上述流程编排能力。**（提供服务具备以上能力的证明材料并盖章）** |

打“★"号条款为实质性条款，若有任何一条负偏离或不满足则导致响应无效。

标的名称：弱电运维服务

| 序号 | 参数性质 | 技术参数与性能指标 |
|---|---|---|
| | • | |

| 序号 | | 具体技术（参数）要求 | |
|---|---|---|---|
| 1 | √ | 响应服务时间需求 | 收到医院保修电话或通知，驻场服务人员要第一时间到达，并展开排查工作；如驻场人员1小时内无法及时解决故障，必须上报公司，公司在2小时内安排故障排查小组入驻；<br>一级故障：影响整体子系统运行的或涉及重点业务区域内的网络系统故障，应在接到报修通知30分钟内恢复，属重大技术问题的，要在1小时内修复，如不能修复的，要给予合理解释，并约定修复期限。<br>二级故障：办公楼区域内的监控、门禁、报警系统的各别点位故障，但不影响系统运行的，应在报修通知8个小时内恢复，如需跟换设备，需与甲方约定到货更换日期。<br>三级故障：楼内的信息发布、楼宇自控、大屏幕等日常办公使用的系统各别点位故障，但不影响系统运行的，应在报修通知24小时内恢复。<br>经维护检测属设备损坏无法维修的，维保人员在规定时间内完成设备配件更换工作。<br>7×24小时提供驻场技术服务。 |
| 2 | √ | 维保人员需求 | 提供≥1名工程师驻场技术7*8小时服务。遇重大会议、活动和季末、年终等节假日重要时间点，可要求临时增派现场维护人员，以保障期间维护工作的顺利进行。 |
| 3 | √ | 技术培训需求 | 按照医院的要求，不定时对系统的操作使用进行现场指导培训或举办专场培训会议。<br>培训目标：对使用操作人员进行应用功能培训，使其能熟练使用系统完成日常业务。<br>培训方法：提供全面技术讲解，通过讲练相结合的教学方式让用户学员学习本系统的操作使用。<br>交付成果：包括但不限于《设备使用说明书》、《使用方法文档截图》、录制培训视频等。 |

1

| | | | | | |
|---|---|---|---|---|---|
| | | 4 | √ | 定期巡检、保养服务需求 | 按国家有关规范和要求派专业人员对系统定期检查、测试、保养、维修、确保设备正常运行。<br>1、每季度对维保项目内的系统和主要设备进行≥1次综合检查工作，对系统和主要设备的运行情况做详细的检查测试，如发现问题第一时间通知相关使用管理部门，并提出合理化解决方案。<br>2、对指定的设备做定期维护保养，包括：系统软件、必要的机械设备、电子部件的除尘清洗，定期保养至少每半年1次。<br>3、每个月对系统软件的数据文件至少进行备份1次。<br>4、维保单位应向医院主管部门提交详细的工作计划与工作安排，对每次巡检、保养工作做好记录，并移交相关负责人签字；<br>5、具体巡查维护次数如下：<br>1）按周巡检：会议室配电系统、视频监控系统、门禁系统、LED大屏、UPS电源系统、精密空调、机房环境监控系统的巡检记录。<br>2）按月巡检：扩声系统、数字IP网络广播系统、综合布线及信息网络维护、护理呼叫系统、分诊排队系统与取号叫号设备与系统、时钟系统、入侵报警系统、电子巡更管理系统、安防设备及系统、智能照明系统、信息发布平台与设备的巡检。<br>3）按季度巡检：弱电井柜、智能AP电源、楼层交换机的巡检的关键数据的备份情况并形成巡检报告。<br>4）按每半年维保：弱电井除尘、数据机房除尘并形成巡检报告。 |
| | | 5 | √ | 配件更换服务 | 提供弱电系统相关配件（包括但不限于安防设备、监控设备、叫号设备等），年度总费用上限为人民币贰拾万元整（¥200,000），由服务方承担；若实际费用超出该限额，超出部分经院方书面确认后由医院据实支付。服务商需按月提供费用明细供甲方审核，未经医院同意的超额支出由服务商自行承担。 |
| 打“★"号条款为实质性条款，若有任何一条负偏离或不满足则导致响应无效。 | | | | | |

标的名称：等级保护测评服务

| 序号 | 参数性质 | 技术参数与性能指标 |
|---|---|---|

<table>
<tr><td>1</td><td></td><td>
<table>
<tr><td>序号</td><td>具体技术（参数）要求</td></tr>
<tr><td>1</td><td>√1.由项目中标人委托测评机特需按照等级保护2.0的相关标准及要求对本项目中要求测评的系统进行测评服务。供应商委托的测评机构须具备由公安部颁发的《网络安全等级测评与检测评估机构服务认证证书》。针对上级部门抽查发现中标供应商提供的等级保护测评报告存在的风险问题，供应商须配合本院，对上级要求整改及书面说明的事项完成整改、情况说明，并出具对应问题专项说明报告。<br>√2.测评依据包括：根据等保安全法《信息安全技术网络安全等级保护基本要求》GB/T22239-2019、（信息安全技术网络安全保护等级定级指南）GB/T22240、《信息安全技术网络安全等级保护实施指南》GB/T25058、《信息安全技术网络安全等级保护剥评要求》GB/T28448-2019、《信息安全技术网络安全等级保护测评过程指南》GB/T28449-2018。对医院≥7个三级业务系统（HIS、LIS、PACS、电子病历系统、集成平台、互联网医院、门户网站）测评，并取得对应系统的网络安全等级保护测评报告。</td></tr>
</table>
</td></tr>
<tr><td colspan="3">打“★"号条款为实质性条款，若有任何一条负偏离或不满足则导致响应无效。</td></tr>
</table>

标的名称：国产化服务器操作系统订阅租用服务

<table>
<tr><td>序号</td><td>参数性质</td><td>技术参数与性能指标</td></tr>
<tr><td>1</td><td></td><td>
<table>
<tr><td>序号</td><td>具体技术（参数）要求</td></tr>
<tr><td>1</td><td>√支持AMD64、ARM64、Mips64、SW64、LoongArch CPU架构；支持飞腾、鲲鹏、海光、兆芯、龙芯、申威等品牌CPU芯片;</td></tr>
<tr><td>2</td><td>√系统支持AppStream应用程序流，支持相同组件多版本并存;</td></tr>
<tr><td>3</td><td>√系统内置国密算法，支持基于国密算法的加解密应用，支持国密SM2/3/4；系统基础组件OpenSSL、Libgcrypt、Gnulib、Nettle、Hashes、libkcapi等支持国密算法;</td></tr>
<tr><td>4</td><td>√提供同品牌自研API网关软件，提供证明;</td></tr>
<tr><td>5</td><td>√支持与操作系统原厂商同品牌的Linux系统通用压力分析套件软件;</td></tr>
<tr><td>6</td><td>√免费提供同品牌自研浏览器，提供功能截图;</td></tr>
<tr><td>7</td><td>√支持自研浏览器软件，且浏览器产品满足GM/T 0087《浏览器密码应用接口规范》、GM/T 0028《密码模块安全技术要求》、GB/T 38636《信息安全技术传输层密码协议（TLCP）》等规范标准</td></tr>
<tr><td>8</td><td>√数量要求：≥88套</td></tr>
</table>
</td></tr>
</table>

打“★"号条款为实质性条款，若有任何一条负偏离或不满足则导致响应无效。

标的名称：网络和数据安全服务

<table>
<tr><th>序号</th><th>参数性质</th><th>技术参数与性能指标</th></tr>
<tr><td></td><td></td><td>
<table>
<tr><th>服务分类</th><th>序号</th><th></th><th>服务名称</th><th>服务参数</th></tr>
<tr><td></td><td>1.1</td><td>√</td><td>网络安全自查自检</td><td>对照自治区卫生健康委、网信部门年度网络安全检查要求及检查指标，结合医院年度网络安全工作计划，制定自查工作方案，明确自查依据、自查内容、自查范围、人员分工与时间进度；对照检查表逐项开展核查（包括但不限于网络与信息系统资产、网络边界与访问控制、安全设备策略及有效性、账号权限与口令、日志审计留存、漏洞与补丁、数据备份与恢复、应急预案与演练、外包及供应链管理等），提前发现并整改问题。<br>服务频次：每年开展2次。上半年场次于3月启动，4月底前完成；下半年场次于8月启动，9月上旬完成。具体开展时间由采购人根据上级检查安排调整，服务商须在主管部门和网信、网安部门检查期间配合现场核查与问题答复。<br>服务交付物：《网络安全自查自检工作方案》《网络安全自查自检问题汇总清单》《重要信息系统清单》《问题整改台账》《网络安全自查自检报告》。</td></tr>
<tr><td></td><td>1.2</td><td>√</td><td>漏洞扫描</td><td>按照自治区中医医院的网络安全全年度工作计划并结合自治区中医医院提供的系统清单，在取得合法授权情况下，对重要在用信息系统或关键信息基础设施开展漏洞扫描工作，每季度开展一次。<br>服务交付物：按照业务系统输出《业务系统漏洞扫描报告》。</td></tr>
</table>
</td></tr>
</table>

| | | | | | | |
|---|---|---|---|---|---|---|
| | | 1.网络安全服务 | 1.3 | ▲ | 渗透测试 | 按照医院网络安全年度工作计划并结合医院提供的系统清单，在取得合法授权情况下，对重要在用信息系统或关键信息基础设施开展非破坏性渗透测试；测试完成后提供修复建议并开展一次复测验证。<br>系统计数口径：以独立业务系统为计数单位（与网络安全等级保护定级备案的系统口径一致），如HIS、电子病历、集成平台、LIS、PACS、互联网医院等各计为1个业务系统；同一业务系统下承载的多台服务器不重复计数。<br>服务频次：每季度开展1次，每次渗透测试系统数不少于5个，全年不少于20个业务系统。<br>服务交付物：按照业务系统输出《业务系统渗透测试报告》（含漏洞修复建议）、《渗透测试漏洞修复验证报告》。**（提供服务承诺函）** |
| | | | 1.4 | √ | 基线核查 | 按照医院网络安全年度工作计划并结合医院提供的系统清单，在取得合法授权情况下，依据网络安全等级保护基本要求及行业安全基线，对重要在用信息系统及相关设备（操作系统、数据库、中间件、网络设备、安全设备等）开展安全配置基线核查，并跟踪整改复核。<br>服务频次：每季度开展1次。<br>服务交付物：按照业务系统输出《业务系统基线核查报告》（含整改建议与复核结论）。 |
| | | | 1.5 | √ | 安全加固 | 结合《网络安全自查自检问题汇总清单》《业务系统漏洞扫描报告》《业务系统渗透测试报告》《业务系统基线核查报告》以及上级监管单位的各类整改通知，对存在的网络安全风险漏洞进行安全加固与整改复验，每季度开展一次。<br>服务交付物：输出《业务系统加固整改报告》。 |
| | | | 1.6 | √ | 应急演练 | 对照自治区中医医院网络安全事件应急预案，组织开展一次网络安全事件应急演练；根据自治区中医医院确定的网络安全事件应急演练时间，制定演练工作方案，明确演练方式、选定场景、演练脚本、模拟环境搭建等；演练结束后形成经验总结，并及时修订完善预案，每年开展一次。<br>提供至少 1 次网络攻防演练配套服务，含演练期间现场值守与技术保障。<br>服务交付物：包括输出《网络安全事件应急演练工作方案》《网络安全事件应急演练脚本》等。 |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 1 | | | | 1.7 | √ | 培训 | 面向医院信息部门技术人员开展技能提升型专业培训，采用理论讲解与实操/案例相结合的方式，由具备中级以上职称技能的资深工程师或行业专家授课；培训方向包括但不限于：安全设备（防火墙、IPS、WAF、堡垒机、日志审计等）配置与运维、网络与业务访问策略设计与优化、漏洞扫描与渗透测试实操、日志分析与安全事件应急处置、等级保护测评要点、数据安全与个人信息保护技术要求、基础环境运维、操作系统运维等方面技能，具体培训内容采购人可根据实际需求进行培训内容调整。<br>服务频次：每年不少于2次，每次培训时长不少于3小时（半天），具体开展时间由采购人指定。<br>服务交付物：《专业技能培训方案与课件》《培训签到与考核记录》《培训总结》。 |
| | | | | 1.8 | √ | 信息化资产梳理 | 对本地（院内机房）在用的信息化资产开展全面调研，重点覆盖网络安全设备（防火墙、IPS/WAF、堡垒机、日志审计、数据库审计、准入控制、网闸等），并可根据采购人需要纳入服务器、存储、虚拟化及网络设备，建立统一资产台账，逐项登记设备名称、品牌型号、数量、部署位置、主要用途、投用时间、软件版本、授权/License/特征库/维保有效期、当前运行状态、责任人等信息；在台账基础上开展资产风险与生命周期评估：①梳理授权已到期、即将到期的设备清单并明确到期时间；②区分可通过续订授权（更新License、特征库、维保服务）解决的项，与厂商已停止支持、授权无法更新需更换设备的项；③提出版本升级、功能替代与设备更换建议；④形成下一年度网络安全建设与预算申报建议，供采购人上会决策和立项参考。<br>说明：云上资源为租用方式，其资产及授权续期纳入上云项目统一考虑，不纳入本地资产台账，服务期间需提供租用的安全设备台账。<br>服务频次：每年开展1次（下半年6-8月份开展，形成下一年度预算依据）。<br>服务交付物：《本地信息化资产台账》（含授权及维保到期情况）、《本地信息化资产风险评估与处置建议报告》（含已到期清单、临期清单、续订授权建议、需更换设备建议及预算测算依据）。 |

| | | | | | | |
|---|---|---|---|---|---|---|
| | | | 1.9 | √ | 业务安全策略优化 | 面向云上及本地网络与业务访问策略开展优化：开展业务访问关系调研、策略现状梳理与风险评估、策略优化设计、策略实施与启用（采用先观察后启用的灰度方式，落实配置备份与回退预案，在业务低峰时段实施并双人复核）、业务验证、持续优化与固化，同步维护策略台账。<br>服务频次：全年不少于2轮全量梳理优化（上、下半年各1轮），每季度开展1次策略巡检与冗余策略清理，重大网络或业务变更后开展专项复核。<br>服务交付物：《网络与业务访问关系调研表》《业务访问关系矩阵》《网络与安全策略现状梳理清单》《策略优化方案》《策略变更实施记录与验证报告》《网络安全策略台账》《策略优化报告》。 |
| | | 2.数据安全服务 | 2.1 | √ | 数据安全风险评估 | 结合《中华人民共和国数据安全法》以及《中华人民共和国个人信息保护法》，基于《网络数据安全风险评估实施指引》对招标方的数据安全管理情况、数据处理活动情况、数据安全技术应用情况以及个人信息保护情况进行调研评估，对6个（HIS系统、电子病历、集成平台、互联网医院、LIS系统、PACS系统）需评估的系统、平台本身存在安全风险进行识别，识别手段至少应包括漏洞扫描、渗透测试等，最后根据以上内容制作数据安全风险评估服务报告，具体开展时间由采购人指定。<br>服务交付物：《数据安全风险评估服务报告》等。 |
| | | | 2.2 | ▲ | 数据分类分级 | 根据国家和行业对数据分类分级的监管要求，结合现有组织架构，设计数据分类分级管理机构，包含数据分类分级的决策机构和最高责任人、数据分类分级的牵头部门、数据分类分级的实施部门，明确各部门的职责和工作，为开展数据分类分级工作提供组织保障；根据数据情况、业务情况和数据分类分级需求，制定数据分类分级管理办法，明确数据分类分级目标、原则、数据分类分级对象、数据共享开放的类型、原则和流程，以及数据分类分级的监管审计要求等，对6个业务系统（HIS系统、电子病历、集成平台、互联网医院、LIS系统、PACS系统）的数据开展数据分类分级，具体开展时间由采购人指定。<br>服务交付物：《数据分类分级清单》《数据分类分级管理办法》《数据分类分级专项报告》《数据安全分类分级规范》等。**（提供服务承诺函）** |

| | | | | | | |
|---|---|---|---|---|---|---|
| | | | 2.3 | √ | 数据安全制度建设 | 依据国家和行业相关法律法规、合规风险情况、业务需求和实际情况，设计覆盖数据全生命周期和数据运营场景的数据安全管理制度框架体系，为数据安全各项工作开展提供依据支撑，同时规范数据安全应用流程，具体开展时间由采购人指定。<br>服务交付物：输出《数据安全管理办法》《数据运维安全管理制度》《个人信息保护制度》《数据安全应急管理制度》《数据安全应急预案》《密码管理制度》《数据全生命周期安全管理制度》等。 |
| 打“★"号条款为实质性条款，若有任何一条负偏离或不满足则导致响应无效。 | | | | | | |

# 第四章 投标人应当提交的资格、资信证明文件

投标人应提交证明其有资格参加投标和中标后有能力履行合同的相关文件，并作为其投标文件的一部分，所有文件必须真实可靠、不得伪造，否则将按相关规定予以处罚。

一、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。

法人包括企业法人、机关法人、事业单位法人和社会团体法人；其他组织主要包括合伙企业、非企业专业服务机构、个体工商户、农村承包经营户；自然人是指具有完全民事行为能力、能够承担民事责任和义务的公民。如投标人是企业（包括合伙企业），要提供在市场监督管理部门注册的有效“企业法人营业执照”或“营业执照”；如投标人是事业单位，要提供有效的“事业单位法人证书”；投标人是非企业专业服务机构，如律师事务所、会计师事务所，要提供有效的执业许可证等证明文件；如投标人是个体工商户，要提供有效的“个体工商户营业执照”；如投标人是自然人，要提供有效的自然人身份证明。

分公司不是独立法人，不具备政府采购法第二十二条规定的投标人应当具备独立承担民事责任能力的条件。分公司经总公司授权，可以以分公司的名义参加政府采购活动，但其民事责任由总公司承担。

二、财务状况报告，依法缴纳税收和社会保障资金的相关材料（详见资格审查表）。

三、具备履行合同所必需的设备和专业技术能力的证明材料。

四、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。

五、按照招标文件要求，投标人应当提交的其他资格、资信证明文件。

# 第五章 评标

## 一.评标要求

1.评标方法

详见须知前附表

2.评标原则

2.1评标活动遵循客观、公正、审慎的原则，以招标文件和投标文件为评标的基本依据，并按照招标文件规定的评标方法和评标标准进行评标。

2.2具体评标事项由评标委员会负责，并按招标文件规定的办法进行评审。

2.3合格投标人不足三家的，不得评标。

3.评标委员会

由采购人代表和评审专家两部分共5人组成， 其中由评审专家库产生的评审专家4人， 由采购人派出的采购人代表1人。

3.1评标委员会由采购人代表和评审专家组成，成员人数应当为5人及以上单数，其中评审专家不得少于成员总数的三分之二。

3.2评标委员会成员有下列情形之一的，应当回避：

（1）参加采购活动前3年内,与投标人存在劳动关系,或者担任投标人的董事、监事,或者是投标人的控股股东或实际控制人；

（2）与投标人的法定代表人或者负责人有夫妻、直系血亲、三代以内旁系血亲或者近姻亲关系；

（3）与投标人有其他可能影响政府采购活动公平、公正进行的关系。

3.3评标委员会负责具体评标事务，并独立履行下列职责：

（1）审查、评价投标文件是否符合招标文件的商务、技术等实质性要求；

（2）要求投标人对投标文件有关事项作出澄清或者说明；

（3）对投标文件进行比较和评价；

（4）确定中标候选人名单，以及根据采购人委托直接确定中标人；

（5）向采购人、采购代理机构或者有关部门报告评标中发现的违法行为；

（6）法律法规规定的其他职责。

4.澄清

对于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，评标委员会应当以书面形式要求投标人作出必要的澄清、说明或者补正。

投标人的澄清、说明或者补正应当采用书面形式，并加盖公章，或者由法定代表人或其授权的代表签字。投标人的澄清、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。

4.1评标委员会不接受投标人主动提出的澄清、说明或补正。

4.2评标委员会对投标人提交的澄清、说明或补正有疑问的，可以要求投标人进一步澄清、说明或补正。

5.有下列情形之一的，视为投标人串通投标，其投标无效：

（1）不同投标人的投标文件由同一单位或者个人编制，包括但不限于不同投标人上传的投标文件项目内部识别码一致的情形；

（2）不同投标人委托同一单位或者个人办理投标事宜；

（3）不同投标人的投标文件载明的项目管理成员或者联系人员为同一人；

（4）不同投标人的投标文件异常一致或者投标报价呈规律性差异；

（5）不同投标人的投标文件相互混装；

（6）不同投标人的投标保证金从同一单位或个人的账户转出；

6.有下列情形之一的，属于恶意串通投标，其投标无效，并追究法律责任：

（1）投标人直接或者间接从采购人或者采购代理机构处获得其他投标人的相关情况并修改其投标文件；

（2）投标人按照采购人或者采购代理机构的授意撤换、修改投标文件；

（3）投标人之间协商报价、技术方案等投标文件的实质性内容；

（4）属于同一集团、协会、商会等组织成员的投标人按照该组织要求协同参加政府采购活动；

（5）投标人之间事先约定由某一特定投标人中标、成交；

（6）投标人之间商定部分投标人放弃参加政府采购活动或者放弃中标、成交；

（7）投标人与采购人或者采购代理机构之间、投标人相互之间，为谋求特定投标人中标、成交或者排斥其他投标人的其他串通行为。

7.投标无效的情形

投标人存在下列情况之一的，投标无效:

（1）未按照招标文件的规定提交投标保证金的；

（2）投标文件未按招标文件要求签署、盖章的；

（3）不具备招标文件中规定的资格要求的；

（4）报价超过招标文件中规定的预算金额或者最高限价的；

（5）投标文件含有采购人不能接受的附加条件的；

（6）法律、法规和招标文件规定的其他无效情形。

8.废标的情形

出现下列情形之一的，应予以废标。

（1）符合专业条件的投标人或者对招标文件作实质响应的投标人不足3家；或参与竞争的核心产品品牌不足3个的；

（2）出现影响采购公正的违法、违规行为的；

（3）投标人的报价均超过了采购预算的；

（4）因重大变故，采购任务取消的；

9.定标

评标委员会按照招标文件确定的评标方法、步骤、标准，对投标文件进行评审。评标结束后，评标委员会根据采购人委托直接确定中标人或者由采购人在评标报告确定的中标候选人名单中按顺序确定中标人。

## 二.落实政府采购政策

1.节约能源、保护环境

采购的产品属于品目清单范围的，将依据国家确定的认证机构出具的、处于有效期之内的节能产品、环境标志产品认证证书，对获得证书的产品实施政府优先采购或强制采购，具体按照本招标文件相关要求执行。

2.促进中小企业发展

2.1采购人在政府采购活动中应当通过加强采购需求管理，落实预留采购份额、价格评审优惠、优先采购等措施，提高中小企业在政府采购中的份额，支持中小企业发展。

2.2《政府采购促进中小企业发展管理办法》所称中小企业，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。符合中小企业划分标准的个体工商户，在政府采购活动中视同中小企业。

2.3在政府采购活动中，投标人提供的货物、工程或者服务符合下列情形的，享受《政府采购促进中小企业发展管理办法》规定的中小企业扶持政策：

（1）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；

（2）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；

（3）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，投标人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《政府采购促进中小企业发展管理办法》规定的中小企业扶持政策。

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。

2.4依照《政府采购促进中小企业发展管理办法》《关于政府采购支持监狱企业发展有关问题的通知》和《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》的规定，凡符合要求的小型、微型企业、监狱企业或残疾人福利性单位，按照以下比例给予相应的价格扣除:

采购包1:

| 序号 | 评审内容 | 适用情形 | 扣除比例 | 具体标准和要求 | 关联投标（响应）文件格式文件 |
|---|---|---|---|---|---|
| 无 | | | | | |

2.5在政府采购活动中，提供货物、工程或者服务符合享受中小企业扶持政策的，投标人应提供《中小企业声明函》；属于监狱企业的，应提供由省级以上监狱管理局、戒毒管理局（含新疆生产建设兵团）出具的属于监狱企业的证明文件；属于残疾人福利性单位的，应提供《残疾人福利性单位声明函》。投标人应当按照《中小企业声明函》《残疾人福利性单位声明函》规定格式提供（格式附后，不可修改），未按规定提供的，不得享受相关中小企业扶持政策。

投标人应当对提供材料的真实性负责，若有虚假，将追究其法律责任。

3.对本国产品的支持政策的相关要求

3.1按照《国务院办公厅关于在政府采购中实施本国产品标准及相关政策的通知》（国办发〔2025〕34号）、《关于贯彻落实《国务院办公厅关于在政府采购中实施本国产品标准及相关政策的通知》的意见》（财库〔2025〕30号）相关要求，本国产品标准适用于货物，包括政府采购货物项目和服务项目中涉及的货物。适用本国产品标准的货物具体是指《政府采购品目分类目录》中的货物类产品，但不包括其中的房屋和构筑物，文物和陈列品，图书和档案，特种动植物，农林牧渔业产品，矿与矿物，电力、城市燃气、蒸汽和热水、水，食品、饮料和烟草原料，无形资产。

本国产品应当在中国境内生产，即在中华人民共和国关境内实现从原材料、组件到产品的属性改变。从具体情形看，在国内保税区、综合保税区等海关特殊监管区域生产的产品，属于在中国境内生产的产品；对医疗器械产品，取得药品监督管理部门授予的准字号医疗器械注册证的，属于在中国境内生产的产品；对其他产品，根据实际情况判断是否在中国境内生产。

3.2政府采购活动中既有本国产品又有非本国产品参与竞争的，依法对本国产品给予价格评审优惠，对本国产品的报价给予20%的价格扣除，用扣除后的价格参与评审。

当采购项目或者采购包中含有多种产品，供应商为该采购项目或者采购包提供的符合本国产品标准的产品成本之和占该供应商提供的全部产品成本之和的比例达到80%以上时，依法对该供应商提供的全部产品给予价格评审优惠，即对该供应商提供的全部产品的总报价给予20%的价格扣除，使用扣除后的价格参与评审。

3.3供应商出具符合要求的《关于符合本国产品标准的声明函》、《本国产品成本比例声明表》（格式附后，不可修改）或有关证明文件的，该产品视为本国产品，采购人、采购代理机构不得再要求供应商提供其他证明材料。供应商提供虚假《关于符合本国产品标准的声明函》、《本国产品成本比例声明表》、虚假证明文件谋取中标、成交的，依照《中华人民共和国政府采购法》等法律法规规定追究相应责任。

符合本国产品的支持政策的相关要求的，按照以下比例进行扣除:

采购包1:

| 序号 | 评审内容 | 适用情形 | 扣除比例 | 具体标准和要求 | 关联投标（响应）文件格式文件 |
|---|---|---|---|---|---|
| 无 | | | | | |

三.评标程序

1.符合性审查

1.1依据招标文件的规定，从投标文件的有效性、完整性和对招标文件的响应程度进行审查，以确定是否满足招标文件的实质性要求。

1.2符合性审查中有任意一项未通过的，审查结果为未通过。投标人未通过符合性审查的，投标无效。

**符合性审查表**

采购包1：2026年业务上云运维服务

| 序号 | 符合审查要求概况 | 评审点具体描述 |
|---|---|---|
| 1 | 投标及保证金缴纳情况 | 按要求进行网上投标、进行保证金缴纳。（审查汇款凭证） |
| 2 | 投标报价 | 投标报价（包括分项报价，投标总报价）只能有一个有效报价且不超过采购预算或最高限价，投标报价不得缺项、漏项。 |
| 3 | 投标文件规范性、符合性 | 投标文件的签署、盖章、涂改、删除、插字、公章使用等符合招标文件要求； |
| 4 | 主要商务条款 | 审查投标人出具的“满足主要商务条款的承诺书”，且进行盖章。 |
| 5 | 技术部分实质性内容 | 1.明确所投标的的服务内容； 2.投标文件应当对招标文件提出的要求和条件作出明确响应并满足招标文件全部实质性要求。 |
| 6 | 其他要求 | 招标文件要求的其他无效投标情形；围标、串标和法律法规规定的其它无效投标条款。 |

2.投标报价审查

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，应当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.政府采购政策功能落实

对于小型、微型企业、监狱企业或残疾人福利性单位给予价格扣除。

4.相同品牌审查

采用最低评标价法的采购项目，提供相同品牌产品的不同投标人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投标人，招标文件未规定的采取随机抽取方式确定，其他投标无效。

使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、符合性审查的不同投标人参加同一合同项下投标的，按一家投标人计算，评审后得分最高的同品牌投标人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投标人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，其他同品牌投标人不作为中标候选人。

多家投标人提供的核心产品品牌相同的，按上述规定处理。

5.详细评审

采购包1：

采购包1：

| 评审内容 | | 评审标准 | | | |
|---|---|---|---|---|---|
| 分值构成 | | 技术部分75.00分<br>商务部分15.00分<br>报价得分10.00分 | | | |
| 评审因素分类 | 评审内容 | 具体标准和要求 | 分值 | 客观/主观 | 关联投标（响应）文件格式文件 |

| | | | | | |
|---|---|---|---|---|---|
| | 技术参数满足情况 | 根据招标文件中“具体技术(参数)要求” 的各项要求的响应情况进行评分：标记“★”为核心技术指标（共计1项），负偏离按无效投标处理；标记“▲”为重要技术指标（共计35项），每负偏离1项扣0.32分，最多扣11.2分； 标记“√”为一般技术指标（共计176项），每负偏离1项扣0.08分，最多扣14.08分。本项合计25.28分，扣完为止。 参数说明：技术参数中明确需提供相关佐证材料的，投标人须提供相应佐证材料，根据投标人提供的技术偏离表及佐证材料进行评审，未提供对应佐证材料的不得分，技术偏离表与佐证材料不一致，以佐证材料为准进行评审。技术参数未要求提供佐证材料的以技术偏离表进行评审。 | 25.2800 | 客观 | 封面<br>目录<br>投标人（供应商）应提交的相关证明<br>投标人业绩情况表<br>投标人基本情况表<br>具备履行合同所必需设备和专业技术能力的声明函<br>主要商务要求承诺书<br>具有良好的商业信誉和健全的财务会计制度的相关材料<br>技术偏离表<br>具有独立承担民事责任的能力证明文件<br>联合体协议<br>项目实施方案、质量保证及售后服务承诺<br>投标人承诺函<br>依法缴纳税收和社会保障资金的良好记录的相关材料<br>项目组成人员一览表<br>中小企业声明函<br>参加政府采购活动前三年内在经营活动中没有重大违法记录的书面声明<br>缴纳投标保证金证明材料<br>其他材料<br>法定代表人授权委托书<br>监狱企业证明文件<br>残疾人福利性单位声明函 |
| | | | | | |

| | | | | |
|---|---|---|---|---|
| 服务方案 | 根据对采购人整体项目的理解程度，提供服务方案，内容包含：1.服务内容质量保障措施、2.服务计划、3.服务流程、4.巡检方案、5.服务时效、6.服务成果等；以上每1项得2.5分，6项合计最高得15分。每项内容缺项，该项不得分。每项内容中每存在一处缺陷扣0.5分，单项扣完为止。（注：“缺陷”指以下任意一种情形：内容不切合行业实际、不符合国家法规政策；或内容凭空编造，与实际情况不符，存在偏差；或内容过于简略；或存在与项目无关的文字内容；或内容不适用项目实际情况；或内容逻辑漏洞；或原理错误；或地点区域错误；或套用其他项目方案；或前后内容互相矛盾；或专业领域知识阐述有误。） | 15.0000 | 主观 | 封面<br>目录<br>投标人（供应商）应提交的相关证明<br>投标人业绩情况表<br>投标人基本情况表<br>具备履行合同所必需设备和专业技术能力的声明函<br>主要商务要求承诺书<br>具有良好的商业信誉和健全的财务会计制度的相关材料<br>技术偏离表<br>具有独立承担民事责任的能力证明文件<br>联合体协议<br>项目实施方案、质量保证及售后服务承诺<br>投标人承诺函<br>依法缴纳税收和社会保障资金的良好记录的相关材料<br>项目组成人员一览表<br>中小企业声明函<br>参加政府采购活动前三年内在经营活动中没有重大违法记录的书面声明<br>缴纳投标保证金证明材料<br>其他材料<br>法定代表人授权委托书<br>监狱企业证明文件<br>残疾人福利性单位声明函 |
| | | | | |

| | | | | | |
|---|---|---|---|---|---|
| | 硬件运维方案 | 根据对采购人整体项目的理解程度，提供硬件运维方案，内容包含：1.运维管理工具、2.常态巡检与针对性维护保养、3.硬件故障排查、4.运维质量保障措施、5.运维服务报告与分析等内容；以上每1项得2分，5项合计最高得10分。每项内容缺项，该项不得分。每项内容中每存在一处缺陷扣0.5分，单项扣完为止。（注：“缺陷”指以下任意一种情形：内容不切合行业实际、不符合国家法规政策；或内容凭空编造，与实际情况不符，存在偏差；或内容过于简略；或存在与项目无关的文字内容；或内容不适用项目实际情况；或内容逻辑漏洞；或原理错误；或地点区域错误；或套用其他项目方案；或前后内容互相矛盾；或专业领域知识阐述有误。） | 10.0000 | 主观 | 封面<br>目录<br>投标人（供应商）应提交的相关证明<br>投标人业绩情况表<br>投标人基本情况表<br>具备履行合同所必需设备和专业技术能力的声明函<br>主要商务要求承诺书<br>具有良好的商业信誉和健全的财务会计制度的相关材料<br>技术偏离表<br>具有独立承担民事责任的能力证明文件<br>联合体协议<br>项目实施方案、质量保证及售后服务承诺<br>投标人承诺函<br>依法缴纳税收和社会保障资金的良好记录的相关材料<br>项目组成人员一览表<br>中小企业声明函<br>参加政府采购活动前三年内在经营活动中没有重大违法记录的书面声明<br>缴纳投标保证金证明材料<br>其他材料<br>法定代表人授权委托书<br>监狱企业证明文件<br>残疾人福利性单位声明函 |
| 技术评审 | | | | | |

| | | | | | |
|---|---|---|---|---|---|
| 技术评审 | 应急保障措施 | 根据对采购人整体项目的理解程度，提供应急保障措施方案，内容包含：1.应急保障组织机构、2.应急运维管理制度、3.应急预案、4.应急响应时效保障、5.应急事件处置方案、6.常用应急备件或配件储备等；以上每1项得1.5分，6项合计最高得9分。每项内容缺项，该项不得分。每项内容中每存在一处缺陷扣0.5分，单项扣完为止。（注：“缺陷”指以下任意一种情形：内容不切合行业实际、不符合国家法规政策；或内容凭空编造，与实际情况不符，存在偏差；或内容过于简略；或存在与项目无关的文字内容；或内容不适用项目实际情况；或内容逻辑漏洞；或原理错误；或地点区域错误；或套用其他项目方案；或前后内容互相矛盾；或专业领域知识阐述有误。） | 9.0000 | 主观 | 封面<br>目录<br>投标人（供应商）应提交的相关证明<br>投标人业绩情况表<br>投标人基本情况表<br>具备履行合同所必需设备和专业技术能力的声明函<br>主要商务要求承诺书<br>具有良好的商业信誉和健全的财务会计制度的相关材料<br>技术偏离表<br>具有独立承担民事责任的能力证明文件<br>联合体协议<br>项目实施方案、质量保证及售后服务承诺<br>投标人承诺函<br>依法缴纳税收和社会保障资金的良好记录的相关材料<br>项目组成人员一览表<br>中小企业声明函<br>参加政府采购活动前三年内在经营活动中没有重大违法记录的书面声明<br>缴纳投标保证金证明材料<br>其他材料<br>法定代表人授权委托书<br>监狱企业证明文件<br>残疾人福利性单位声明函 |
| | | | | | |

| | | | | |
|---|---|---|---|---|
| 数据迁移方案 | 根据对采购人整体项目的理解程度，提供数据迁移方案，内容包含1.前期准备与现状分析、2.数据迁移技术应用、3.具体实施计划、4.业务切换与割接方案、5.数据安全与保密措施、6.迁移文档与成果交付；以上每1项得2分，6项合计最高得12分。每项内容缺项，该项不得分。每项内容中每存在一处缺陷扣0.5分，单项扣完为止。（注：“缺陷”指以下任意一种情形：内容不切合行业实际、不符合国家法规政策；或内容凭空编造，与实际情况不符，存在偏差；或内容过于简略；或存在与项目无关的文字内容；或内容不适用项目实际情况；或内容逻辑漏洞；或原理错误；或地点区域错误；或套用其他项目方案；或前后内容互相矛盾；或专业领域知识阐述有误。） | 12.0000 | 主观 | 封面<br>目录<br>投标人（供应商）应提交的相关证明<br>投标人业绩情况表<br>投标人基本情况表<br>具备履行合同所必需设备和专业技术能力的声明函<br>主要商务要求承诺书<br>具有良好的商业信誉和健全的财务会计制度的相关材料<br>技术偏离表<br>具有独立承担民事责任的能力证明文件<br>联合体协议<br>项目实施方案、质量保证及售后服务承诺<br>投标人承诺函<br>依法缴纳税收和社会保障资金的良好记录的相关材料<br>项目组成人员一览表<br>中小企业声明函<br>参加政府采购活动前三年内在经营活动中没有重大违法记录的书面声明<br>缴纳投标保证金证明材料<br>其他材料<br>法定代表人授权委托书<br>监狱企业证明文件<br>残疾人福利性单位声明函 |

| | | | | | |
|---|---|---|---|---|---|
| | 培训方案 | 根据对采购人整体项目的理解程度，提供培训方案，内容包含1.培训计划和培训内容、2.培训师资和培训目标等；以上每1项得1.86分，2项合计最高得3.72分。每项内容缺项，该项不得分。每项内容中每存在一处缺陷扣0.5分，单项扣完为止。（注：“缺陷”指以下任意一种情形：内容不切合行业实际、不符合国家法规政策；或内容凭空编造，与实际情况不符，存在偏差；或内容过于简略；或存在与项目无关的文字内容；或内容不适用项目实际情况；或内容逻辑漏洞；或原理错误；或地点区域错误；或套用其他项目方案；或前后内容互相矛盾；或专业领域知识阐述有误。） | 3.7200 | 主观 | 封面<br>目录<br>投标人（供应商）应提交的相关证明<br>投标人业绩情况表<br>投标人基本情况表<br>具备履行合同所必需设备和专业技术能力的声明函<br>主要商务要求承诺书<br>具有良好的商业信誉和健全的财务会计制度的相关材料<br>技术偏离表<br>具有独立承担民事责任的能力证明文件<br>联合体协议<br>项目实施方案、质量保证及售后服务承诺<br>投标人承诺函<br>依法缴纳税收和社会保障资金的良好记录的相关材料<br>项目组成人员一览表<br>中小企业声明函<br>参加政府采购活动前三年内在经营活动中没有重大违法记录的书面声明<br>缴纳投标保证金证明材料<br>其他材料<br>法定代表人授权委托书<br>监狱企业证明文件<br>残疾人福利性单位声明函 |

| | | | | | |
|---|---|---|---|---|---|
| 商务评审 | 业绩 | 自2023年1月到至投标截止时间，投标人具有类似业绩案例，以合同关键页为准（需包含合同首页、清单及盖章页），每提供一个案例得2分，满分10分。提供案例证明文件复印件并加盖投标人公章。 | 10.0000 | 客观 | 封面<br>目录<br>投标人（供应商）应提交的相关证明<br>投标人业绩情况表<br>投标人基本情况表<br>具备履行合同所必需设备和专业技术能力的声明函<br>主要商务要求承诺书<br>具有良好的商业信誉和健全的财务会计制度的相关材料<br>技术偏离表<br>具有独立承担民事责任的能力证明文件<br>联合体协议<br>项目实施方案、质量保证及售后服务承诺<br>投标人承诺函<br>依法缴纳税收和社会保障资金的良好记录的相关材料<br>项目组成人员一览表<br>中小企业声明函<br>参加政府采购活动前三年内在经营活动中没有重大违法记录的书面声明<br>缴纳投标保证金证明材料<br>其他材料<br>法定代表人授权委托书<br>监狱企业证明文件<br>残疾人福利性单位声明函 |

| | | | | | |
|---|---|---|---|---|---|
| 商务评审 | 人员配备 | 投标人为本项目配置的驻场服务团队：1.项目经理具备信息系统管理工程师（高级）证书，提供得2分，不提供不得分；2.项目团队组成员中具备中级及以上职称的注册信息安全工程师证书、网络工程师、信息系统项目管理师，每有一个证书得1分，一人多证只计一次分，最高得3分，不提供不得分； | 5.0000 | 客观 | 封面<br>目录<br>投标人（供应商）应提交的相关证明<br>投标人业绩情况表<br>投标人基本情况表<br>具备履行合同所必需设备和专业技术能力的声明函<br>主要商务要求承诺书<br>具有良好的商业信誉和健全的财务会计制度的相关材料<br>技术偏离表<br>具有独立承担民事责任的能力证明文件<br>联合体协议<br>项目实施方案、质量保证及售后服务承诺<br>投标人承诺函<br>依法缴纳税收和社会保障资金的良好记录的相关材料<br>项目组成人员一览表<br>中小企业声明函<br>参加政府采购活动前三年内在经营活动中没有重大违法记录的书面声明<br>缴纳投标保证金证明材料<br>其他材料<br>法定代表人授权委托书<br>监狱企业证明文件<br>残疾人福利性单位声明函 |

| | | | | | |
|---|---|---|---|---|---|
| 价格评审 | 价格评审 | F1指价格项评审因素得分＝（评标基准价/投标报价）×100×价格项评审因素所占的权重（注：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。）最低报价不是中标的唯一依据。因落实政府采购政策进行价格调整的，以调整后的价格计算评标基准价和投标报价。 | 10.0000 | 客观 | 分项报价表<br>开标一览表 |

价格扣除

| 序号 | 价格扣除评审内容 | 适用情形 | 扣除比例（C1） | 具体标准和要求 | 关联投标（响应）文件格式文件 |
|---|---|---|---|---|---|
| 无 | | | | | |

异常低价审查:

采购包1:

| 序号 | 评审点要求概况 | 异常低价的情形 |
|---|---|---|

| | | |
|---|---|---|
| 1 | 异常低价审查 | 根据《关于推动解决政府采购异常低价问题的通知》（财库〔2026〕2号）等相关规定，政府采购评审中出现下列情形之一的，评审委员会应当启动异常低价投标（响应）审查程序：<br>（1）投标（响应）报价低于全部通过符合性审查供应商投标（响应）报价平均值50%的，即投标（响应）报价<全部通过符合性审查供应商投标（响应）报价平均值×50%。<br>（2）投标（响应）报价低于通过符合性审查且报价次低供应商投标（响应）报价50%的，即投标（响应）报价<通过符合性审查且报价次低供应商投标（响应）报价×50%。<br>（3）投标（响应）报价低于最高限价45%的，即投标（响应）报价<最高限价×45%。<br>（4）评审委员会基于专业判断，认为供应商报价过低，有可能影响产品质量或者不能诚信履约的其他情形。<br>评审委员会启动异常低价投标（响应）审查后，应当要求相关供应商在评审现场合理的时间内对投标（响应）价格作出解释，提供项目具体成本测算等与报价合理性相关的书面说明及必要的证明材料，包括但不限于原材料成本、人工成本、制造费用等，给予相关供应商的合理时间一般不少于30分钟。其中，属于第3项情形，供应商已随投标（响应）文件一并提交相关书面说明及必要的证明材料的，在评审现场可不再重复提交。评审委员会依据专业经验，参考同类项目中标（成交）价格、类似产品市场价格水平、行业人工费用标准、国家有关部门指导行业协会发布的行业平均成本等情况，对报价合理性进行判断。投标（响应）供应商不能提供书面说明、证明材料，或者提供的书面说明、证明材料不能证明其报价合理性的，评审委员会应当将其作为无效投标（响应）处理。 |

6.汇总、排序

最低评标价法：评标结果按投标报价由低到高顺序排列。投标报价相同的并列。投标文件满足招标文件全部实质性要求且投标报价最低的投标人为排名第一的中标候选人。

综合评分法：评标结果按评审后得分由高到低顺序排列。得分相同的，按投标报价由低到高顺序排列。得分且投标报价相同的并列。投标文件满足招标文件全部实质性要求，且按照评审因素的量化指标评审得分最高的投标人为排名第一的中标候选人。

7.确定中标人

采购人或者评标委员会按照中标候选人名单顺序确定中标人。中标候选人并列的，按采购人授权评标委员会按照评审原则直接确定中标（成交）人。招标文件未规定的，采取随机抽取的方式确定。

# 第六章 合同与验收

## 一.合同

1.合同要求

1.1采购人应当自中标（成交）通知书发出之日起30日内，按照招标（磋商、谈判）文件或询价通知书和中标（成交）供应商投标（响应）文件的规定，与中标（成交）供应商签订书面合同。所签订的合同不得对招标（磋商、谈判）文件或询价通知书确定的事项作实质性修改。采购人、供应商不得提出任何不合理的要求作为签订合同的条件。

1.2政府采购合同应当包括采购人与中标（成交）供应商的名称和住所、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。

1.3采购人与中标（成交）供应商应当根据合同的约定依法履行合同义务。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》。政府采购合同的双方当事人不得擅自变更、中止或者终止合同。

1.4采购人应当自政府采购合同签订之日起2个工作日内，将政府采购合同在内蒙古自治区政府采购网（https://www.ccgp-neimenggu.gov.cn/）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。

1.5采购人应当自政府采购合同签订之日起7个工作日内，将合同副本向同级财政部门和有关部门备案。

2.合同内容及格式

# 政府采购合同

## （货物类合同参考文本）

合同编号：

甲方：***（填写采购单位名称）

地址：***（填写详细地址）

乙方：***（填写中标、成交供应商名称）

地址：***（填写详细地址）

根据《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》《中华人民共和国民法典》等相关法律法规、规范性文件以及 _____项目（填写项目名称）_____ （填写政府采购项目编号）的中标（成交）结果、招标（磋商、谈判）文件或询价通知书、投标（响应）文件等文件的相关内容，甲乙双方经平等协商，就如下合同条款达成一致意见。

一、甲方向乙方采购的货物基本情况

（一）根据招标（磋商、谈判）文件或询价通知书及中标（成交）结果公告，甲方所采购的货物、服务（如有）基本情况如下：_____。

（二）货物名称、数量、规格型号、生产厂家、品牌、单价、与货物相关的服务等详细内容，见合同附件-货物清单。

二、乙方交付货物的时间及地点

（一）交付时间：_____

（二）交付地点：_____（填写详细地址）

（三）交付货物的名称及数量：_____

（四）乙方交付货物代表及联系电话：_____（填写姓名和联系电话）

（五）甲方接收货物代表及联系电话：_____（填写姓名和联系电话）

注：货物为多批次交付的，应详细列明每批次交付的内容、数量、交付时间、交付地点等。

三、乙方交付货物的质量

（一）乙方交付的货物应同时满足：1.符合国家法律法规和规范性文件对货物的质量要求；2.符合甲方招标（磋商、谈判）文件或询价通知书对货物的质量要求；3.符合乙方在投标（响应）文件中或磋商、谈判过程中对货物质量作出的书面承诺、声明或保证。上述质量要求作为甲方对乙方货物质量的验收依据。

（二）乙方应根据国家法律法规和规范性文件的规定、招标（磋商、谈判）文件或询价通知书的相关要求、投标（响应）文件及乙方承诺、声明或保证，向甲方提供相应的货物质量证明文件。

四、乙方交付货物的包装及标识

（一）乙方交付货物的包装和标识应同时满足：1.符合国家法律法规和规范性文件对产品包装及标识的要求；2.符合甲方招标（磋商、谈判）文件或询价通知书对货物包装及标识的要求；3.符合乙方在投标（响应）文件中对货物包装及标识作出的承诺、声明或保证；4.符合绿色环保、运输及安全性等要求。

（二）货物的包装费用由乙方承担。

五、货物的运输要求

（一）运输方式及运输线路：_____。

（二）运输、保险及其他相关费用由乙方承担。

六、甲方对货物的验收

（一）乙方将货物送达至甲方指定的地点，应及时通知甲方。在甲方收到到货通知并在货物到达指定地点后_____日

内，由甲乙双方及第三方（如有）对货物的数量、规格型号、生产厂家、品牌、外观进行验收，在条件允许的情况下，可以同步对货物质量进行初步验收，甲乙双方应签署书面验收记录，作为本项目的履行文件留存。

（二）在甲方收到货物_____日内，如发现质量问题，甲方应在_____日内向乙方提出书面异议，甲方逾期提出的，视为乙方所交付的货物质量符合合同的约定。乙方在收到甲方关于质量问题的书面异议后，应当在_____日内负责解决处理。

（三）乙方提交的货物数量、规格型号及质量不符合本合同要求的，甲方应在验收记录中作出明确记载，保留相关的证据，并有权拒绝接受货物，解除合同且不承担任何法律责任。

七、合同金额

在乙方提供完全符合合同要求的货物的前提下，本合同总金额为_____元（小写）_____（大写）

八、付款时间、金额及条件

（一）付款时间及付款金额：_____

（二）付款条件：_____

（三）乙方账户信息

乙方名称：_____

开户银行：_____

银行账号：_____

九、货物质量保证及售后服务

招标（磋商、谈判）文件或询价通知书对货物质量保证期及售后服务作出明确要求的，适用招标（磋商、谈判）文件或询价通知书对保证期和售后服务的规定，如乙方在投标（响应）文件及磋商、谈判过程中对货物质量保证期和售后服务作出更优的承诺、声明或保证的，适用乙方的承诺、声明或保证。

十、知识产权

乙方保证其提供的货物的全部及部分，均不存在任何侵犯第三方知识产权的情形。否则，乙方应向甲方承担违约责任及赔偿由此给甲方造成的名誉及经济损失。

十一、违约条款

（一）甲方没有正当理由逾期支付合同款项的，每延期一日，甲方应按照逾期支付金额_____ 的_____承担违约责任。延期达到_____日，乙方有权解除合同，并要求甲方赔偿由此造成的经济损失。

（二）甲方存在其他违反本合同的行为，应承担相应的违约责任（注：可以根据情况进行细化）；违约金不足以赔偿乙方损失的，乙方有权要求甲方赔偿由此造成的经济损失。

（三）乙方逾期交付货物的，每延期一日，乙方应按照合同总金额的_____承担违约责任。延期达到_____日，甲方有权解除合同，拒付延期部分货物的相应货款，并要求乙方赔偿甲方的经济损失。

（四）乙方交付的货物不符合质量约定或乙方未履行相应的质量保证责任及售后服务义务、或存在侵权行为的，甲方有权退货，并要求乙方支付合同总金额_____%的违约金，违约金不足以赔偿甲方损失的，甲方有权要求乙方赔偿经济损失。

（五）乙方在参与本项目采购活动过程中，如存在提供虚假承诺、证明、串通投标等违法违规行为，除承担相应的行政责任外，甲方有权解除合同，并要求乙方承担合同总金额_____%的违约金，违约金不足以赔偿甲方损失的，甲方有权要求乙方赔偿经济损失。

（六）乙方存在其他违反本合同的行为，应承担相应的违约责任（注：可以根据情况进行细化）；违约金不足以赔偿甲方损失的，甲方有权要求乙方赔偿经济损失。

十二、不可抗力

因不可抗力致使一方不能及时或完全履行合同的，应及时通知另一方，双方互不承担责任，并在_____天内提供有关不可抗力的相关证明。合同未履行部分是否继续履行、如何履行等问题，双方协商解决。

十三、争议的解决方式

合同发生纠纷时，双方应协商解决，协商不成，可以采用下列方式解决：

（一）提交_____仲裁委员会仲裁。

（二）向_____人民法院起诉。

十四、合同保存

合同文本一式_____份，采购单位、中标（成交）供应商、采购代理机构、_____各执一份。合同文本保存期限为从采购结束之日起至少保存十五年。

十五、合同附件

本合同所附下列文件是构成本合同不可分割的组成部分，其内容与本合同具有同等的法律效力：

1、货物清单（双方应盖章确认）

2、乙方出具的报价单（函）

3、中标（成交）结果公告及中标（成交）通知书

4、甲方招标（磋商、谈判）文件或询价通知书

5、乙方投标（响应）文件

6、甲乙双方商定的其他文件

十六、双方约定的其他条款

_____。

十七、本合同未尽事宜，由双方另行签订补充协议，补充协议是本合同的组成部分。

十八、本合同由甲乙双方盖章生效。

甲方名称：（章）

甲方法定代表人或负责人：（签字）

年 月 日

乙方名称：（章）

乙方法定代表人或负责人：（签字）

年 月 日

# 政府采购合同

## （服务类合同参考文本）

合同编号：

甲方：***（填写采购单位名称）

地址：***（填写详细地址）

乙方：***（填写中标、成交供应商名称

地址：***（填写详细地址）

甲乙双方根据《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》《中华人民共和国民法典》等相关法律法规、规范性文件以及_____项目（填写项目名称）_____（填写政府采购项目编号）的中标（成交）结果、招标（磋商、谈判）文件、投标（响应）文件等文件的相关内容，经平等自愿协商一致，就如下合同条款达成一致意见。

一、乙方向甲方提供的服务内容

（一）根据招标（磋商、谈判）文件及中标（成交）结果公告，乙方向甲方提供的服务、货物（如有）内容如下：_____

_____。

（二）服务项目名称、服务具体内容、服务方式、服务要求、服务成果及与之相关的货物等详细内容，见合同附件—服务清单。

二、乙方服务成果的交付时间、地点

（一）服务期限：_____

（二）服务成果的交付时间和交付要求（如有）：_____

（三）服务地点：_____（填写详细地址）

（四）乙方代表及联系电话：_____（填写姓名和联系电话）

（五）甲方代表及联系电话：_____（填写姓名和联系电话）

注：服务成果分阶段交付的，应分别列明各阶段的交付时间、交付内容。

三、乙方提供服务成果的质量

（一）乙方提供的服务应同时满足：1.符合国家法律法规和规范性文件对服务质量的要求；2.符合甲方招标（磋商、谈判）文件对服务的质量要求；3.符合乙方在投标（响应）文件中或磋商、谈判过程中对服务质量作出的书面承诺、声明或保证。上述质量要求作为甲方对乙方服务质量的验收依据。

（二）乙方应根据国家法律法规和规范性文件的规定、招标（磋商、谈判）文件的相关要求、投标（响应）文件及乙方承诺、声明或保证，向甲方提供相应的服务质量证明文件。

四、乙方服务成果的交付方式及载体

乙方交付服务成果方式及载体应符合国家法律法规和规范性文件的要求，并符合甲方招标（磋商、谈判）文件的要求、乙方在投标（响应）文件中对服务成果交付方式及载体作出的承诺。

五、甲方对乙方服务的监督

甲方对乙方提供的服务有权进行监督，当乙方服务质量、服务内容不符合约定时，甲方有权要求乙方及时进行整改，对乙方拒不改正或整改不到位的，甲方有权随时解除合同，并根据具体情况扣除部分或全部服务费用。

六、合同金额

在乙方提供完全符合合同要求的服务的前提下，本合同总金额为_____元（小写）_____（大写）。

七、付款时间及条件

（一）付款时间：_____

（二）付款条件：_____

（三）乙方账户信息

乙方名称：_____

开户银行：_____

银行账号：_____

八、知识产权

乙方应保证其提供的服务及服务成果的全部及部分，均不存在侵犯第三方知识产权的情形，其服务成果的所有权由甲方享有。否则，乙方应向甲方承担违约责任及赔偿由此给甲方造成的名誉及经济损失。

九、违约条款

（一）甲方没有正当理由逾期支付合同款项的，每延期一日，甲方应按照逾期支付金额_____的_____承担违约责任。延期达到_____日，乙方有权解除合同，并要求甲方赔偿由此造成的经济损失。

（二）甲方存在其他违反本合同的行为，应承担相应的违约责任（注：可以根据情况进行细化）；违约金不足以赔偿乙方损失的，乙方有权要求甲方赔偿由此造成的经济损失。

（三）乙方逾期提供服务成果的，每延期一日，乙方应按照合同总金额的_____承担违约责任。延期达到_____日，甲方有权解除合同，拒付延期部分的相应服务款项，并要求乙方赔偿甲方的经济损失。

（四）乙方交付的服务不符合质量要求，或其服务成果存在侵权行为的，甲方有权解除合同，并要求乙方支付合同总金额_____%的违约金，违约金不足以赔偿甲方损失的，甲方有权要求乙方赔偿经济损失。

（五）乙方在参与本项目采购活动过程中，如存在提供虚假承诺、证明、串通投标等违法违规行为，除承担相应的行政责任外，甲方有权解除合同，并要求乙方承担合同总金额_____%的违约金，违约金不足以赔偿甲方损失的，甲方有权要求乙方赔偿经济损失。

（六）乙方存在其他违反本合同的行为，应承担相应的违约责任（注：可以根据情况进行细化）；违约金不足以赔偿甲方损失的，甲方有权要求乙方赔偿经济损失。

十、不可抗力

因不可抗力致使一方不能及时或完全履行合同的，应及时通知另一方，双方互不承担责任，并在_____天内提供有关不可抗力的相关证明。合同未履行部分是否继续履行、如何履行等问题，由双方协商解决。

十一、争议的解决方式

合同发生纠纷时，双方应协商解决，协商不成，可以采用下列方式解决：

（一）提交_____仲裁委员会仲裁。

（二）向_____人民法院起诉。

十二、合同保存

合同文本一式____份，采购单位、中标（成交）供应商、采购代理机构、_____各执一份。合同文本保存期限为从采购结束之日起至少保存十五年。

十三、合同附件

本合同所附下列文件是构成本合同不可分割的部分，与本合同具有同等法律效力：

1、服务清单（双方应盖章确认）

2、乙方出具的报价单（函）

3、中标（成交）结果公告及中标（成交）通知书

4、甲方招标（磋商、谈判）文件

5、乙方投标（响应）文件

6、甲乙双方商定的其他文件

十四、双方约定的其他事宜

_____。

十五、合同未尽事宜，双方另行签订补充协议，补充协议是合同的组成部分。

十六、本合同由甲乙双方盖章生效。

甲方名称：（章）

甲方法定代表人或负责人：（签字）

年 月 日

乙方名称：（章）

乙方法定代表人或负责人：（签字）

年 月 日

# 政府采购合同

## （工程类合同参考文本）

合同编号：

甲方：***（填写采购单位名称）

地址：***（填写详细地址）

乙方：***（填写中标、成交供应商名称

地址：***（填写详细地址）

根据《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》《中华人民共和国民法典》等相关法律法规、规范性文件以及_____项目（填写项目名称）_____填写政府采购项目编号）的成交结果、磋商（谈判）文件、响应文件等文件的相关内容，甲乙双方经平等协商，就如下合同条款达成一致意见。

一、工程项目的基本情况

（一）根据磋商（谈判）文件及成交结果公告，乙方向甲方提供的工程项目及设施设备（如有）、服务（如有）基本情况如下：_____。

（二）工程项目的名称、建设地点、工程技术规范及要求、工程量等具体内容，乙方提供的材料及设备名称、规格型号、品牌、单价、产地以及与工程、材料、设施设备相关的服务等详细内容，见合同附件—工程清单

二、工程建设计划及相应的工期要求

_____。

注：如工程建设分阶段，应详细列明各阶段工程建设内容及工期要求。

三、工程质量要求

（一）乙方建设工程应同时满足：1.符合国家法律法规和规范性文件对工程的质量要求；2.符合甲方磋商（谈判）文件对工程的质量要求；3.符合乙方在响应文件中或磋商、谈判过程中对工程质量作出的书面承诺、声明或保证。上述工程质量要求作为甲方对乙方工程质量的验收依据

（二）乙方应根据国家法律法规和规范性文件的规定、磋商（谈判）文件的相关要求、响应文件及乙方承诺、声明或保证，向甲方提供相应的工程质量满足要求的证明文件。

四、对工程验收的约定

（一）甲乙双方对工程建设过程中的各阶段验收、总验收及乙方提供的材料设备验收的条件和时间约定如下：

_____

注：根据项目具体情况填写。

（二）如乙方未通过甲方组织的各阶段验收，甲方有权要求乙方在限定期限内整改，如整改不合格，甲方有权追究乙方违约责任，解除合同并要求乙方赔偿经济损失。

五、合同金额

在乙方提供完全符合合同要求的工程、材料、设施设备、服务的前提下，本合同总金额为_____元（小写）_____（大写）。

六、付款时间及条件

（一）付款时间：_____

（二）付款条件：_____

（三）乙方账户信息

乙方名称：_____

开户银行：_____

银行账号：_____

七、甲方对乙方工程的监督

甲方及甲方委派的代表有权对乙方工程、材料及设施设备、服务等质量及管理进行监督，当乙方工程质量、材料及设施设备、服务内容不符合约定时，甲方及授权代表有权要求乙方及时进行整改，对乙方拒不改正或整改不到位的，甲方有权随时解除合同，并根据具体情况扣除部分或全部工程费用。

八、质量保证及售后服务

磋商（谈判）文件对工程质量保证期、材料设施设备质保期和售后、服务质量作出明确要求的，适用磋商（谈判）文件对工程质量保证期及材料设施设备质保期和售后、服务质量的规定，如乙方在响应文件及磋商（谈判）过程中对工程质量保证期及设施设备质保期和售后、服务质量作出更优的承诺、声明或保证的，适用乙方的承诺、声明或保证。

九、违约条款

（一）甲方没有正当理由逾期支付合同款项的，每延期一日，甲方应按照逾期支付金额_____的_____承担违约责任。延期达到_____日，乙方有权解除合同，并要求甲方赔偿由此造成的经济损失。

（二）甲方存在其他违反本合同的行为，应承担相应的违约责任（注：可以根据情况进行细化）；违约金不足以赔偿乙方损失的，乙方有权要求甲方赔偿由此造成的经济损失。

（三）乙方逾期交付工程的，每延期一日，乙方应按照合同总金额的_____承担违约责任。延期达到_____日，甲方有权解除合同，拒付延期部分的相应工程款，并要求乙方赔偿甲方经济损失。

（四）乙方交付的工程及设施设备、服务质量不符合质量规定或乙方未履行相应的工程质量保证期及设施设备质保期和售后、服务义务的，甲方有权拒付相应的工程款，并要求乙方支付合同总金额_____%的违约金。违约金不足以赔偿损失的，甲方有权要求乙方赔偿经济损失。

（五）乙方在参与本项目采购活动过程中，如存在提供虚假承诺、证明、串通投标等违法违规行为，除承担相应的行政责任外，甲方有权解除合同，并要求乙方承担合同总金额_____%的违约金，违约金不足以赔偿甲方损失的，甲方有权要求乙方赔偿经济损失。

（六）乙方存在其他违反本合同的行为，应承担相应的违约责任（可以根据情况进行细化）；违约金不足以赔偿甲方损失的，甲方有权要求乙方赔偿经济损失。

十、不可抗力条款

因不可抗力致使一方不能及时或完全履行合同的，应及时通知另一方，双方互不承担责任，并在_____天内提供有关不可抗力的相关证明。合同未履行部分是否继续履行、如何履行等问题，由双方协商解决。

十一、争议的解决方式

合同发生纠纷时，双方应协商解决，协商不成，可以采用下列方式_____解决：

（一）提交_____仲裁委员会仲裁。

（二）向_____人民法院起诉。

十二、合同保存

合同文本一式____份，采购单位、中标（成交）供应商、采购代理机构、_____各执一份。合同文本保存期限为从采购结束之日起至少保存十五年。

十三、合同附件

本合同所附下列文件是构成本合同不可分割的部分，与本合同具有同等法律效力：

1.工程清单（双方应盖章确认）

2.乙方出具的报价单（函）

3.成交结果公告及成交通知书

4.甲方磋商（谈判）文件

5.乙方响应文件

6.甲乙双方商定的其他文件

十四、双方约定的其他事宜

_____。

十五、本合同未尽事宜，双方另行签订补充协议，补充协议是合同的组成部分。

十六、本合同由甲乙双方盖章生效。

甲方名称：（章）

甲方法定代表人或负责人：（签字）

年 月 日

乙方名称：（章）

乙方法定代表人或负责人：（签字）

年 月 日

**二.验收**

严格按照采购合同开展履约验收。采购人或者采购代理机构应当成立验收小组，按照采购合同的约定对投标人履约情况进行验收。验收时，应当按照采购合同的约定对每一项技术、服务、安全标准的履约情况进行确认。验收结束后，应当出具验收书（参考格式附后），列明各项标准的验收情况及项目总体评价，由验收双方共同签署。验收结果应当与采购合同约定的资金支付及履约保证金返还条件挂钩。履约验收的各项资料应当存档备查。

# 政府采购货物履约验收书

（参考格式）

| | |
|---|---|
| 项目名称 | |
| 项目编号 | |
| 采购人 | |
| 使用人 | |
| 供应商 | |
| 验收依据 | 1.政府采购合同（合同名称及编号）<br>2.中标（成交）公告或中标（成交）通知书<br>3.招标（磋商、谈判）文件或询价通知书<br>4.投标（响应）文件<br>5.供应商的承诺、声明或保证（如有）<br>注：验收依据可根据项目具体情况适当增加 |
| 供应商对履约情况的总结及提供的相关证明材料 | 注：供应商根据采购合同的约定，对履约情况（包括但不限于采购合同中约定的货物数量、货物规格型号、生产厂家、交货时间、交货地点、验收情况、货物质量、售后服务等）进行总结，并提供相应的履约证明材料作为附件。 |
| 采购人（使用人）对履约情况的确认 | 注：采购人或使用人根据采购合同约定，对供应商履约情况进行逐一确认。 |
| 验收人员名单及组成 | 1. 采购人代表:<br>2. 采购代理机构代表:<br>3. 第三方专业机构代表及专家:<br>4. 其他供应商代表: |
| 验收评价及结论 | 评价:<br>结论：□通过 □不通过，具体说明: |
| 验收人员签字 | 年 月 日 |
| 采购人确认意见（注:采购人委托代理机构验收时适用） | □同意验收结论。<br>□不同意验收结论。具体说明:<br>年 月 日 |
| 备注 | |

采购人代表签字:

年 月 日

供应商代表签字:

年 月 日

政府采购服务履约验收书

（参考格式）

| | |
|---|---|
| 项目名称 | |
| 项目编号 | |
| 采购人 | |
| 使用人 | |
| 供应商 | |
| 验收依据 | 1.政府采购合同（合同名称及编号）<br>2.中标（成交）公告或中标（成交）通知书<br>3.招标（磋商、谈判）文件或询价通知书<br>4.投标（响应）文件<br>5.供应商的承诺、声明或保证（如有）<br>注：验收依据可根据项目具体情况适当增加 |
| 供应商对履约情况的总结及提供的相关证明材料 | 注：供应商根据采购合同的约定，对履约情况（包括但不限于采购合同中约定的服务内容、服务要求、服务质量、人员配置、服务成果、服务成果的交付等）进行总结，并提供相应的履约证明材料作为附件。 |
| 采购人（使用人）对履约情况的确认 | 注：采购人或使用人根据采购合同约定，对供应商履约情况进行逐一确认。 |
| 验收人员名单及组成 | 1. 采购人代表：<br>2. 采购代理机构代表：<br>3. 第三方专业机构代表及专家：<br>4. 其他供应商代表： |
| 验收评价及结论 | 评价：<br>结论：□通过 □不通过，具体说明： |
| 验收人员签字 | 年 月 日 |
| 采购人确认意见（注：采购人委托代理机构验收时适用） | □同意验收结论。<br>□不同意验收结论。具体说明：<br>年 月 日 |
| 备注 | |

采购人代表签字：

年 月 日

供应商代表签字：

年 月 日

# 政府采购工程履约验收书

（参考格式）

| | |
|---|---|
| 项目名称 | |
| 项目编号 | |
| 采购人 | |
| 使用人 | |
| 供应商 | |
| 验收依据 | 1.政府采购合同（合同名称及编号）<br>2.成交公告及成交通知书<br>3.磋商、谈判文件<br>4.响应文件<br>5.供应商的承诺及保证（如有）<br>6.国家关于工程建设的相关法律法规及规范性文件<br>注：验收依据可根据项目具体情况适当增加 |
| 供应商对履约情况的总结及提供的相关证明材料 | 注：供应商根据采购合同的约定，对履约情况（包括但不限于采购合同中约定的工程内容、工程质量、工程进度、工程各阶段验收、安全管理、材料及设施设备等）进行总结，并提供相应的履约证明材料作为附件。 |
| 采购人（使用人）对履约情况的确认 | 注：采购人或使用人根据采购合同约定，对供应商履约情况进行逐一确认。 |
| 验收人员名单及组成 | 1. 采购人代表：<br>2. 采购代理机构代表：<br>3. 第三方专业机构代表及专家：<br>4. 其他供应商代表： |
| 验收评价及结论 | 评价：<br>结论：□通过 □不通过，具体说明： |
| 验收人员签字 | 年 月 日 |
| 采购人确认意见（注：采购人委托代理机构验收时适用） | □同意验收结论。<br>□不同意验收结论。具体说明：<br>年 月 日 |
| 备注 | |

采购人代表签字：

年 月 日

供应商代表签字：

年 月 日

# 第七章 响应文件格式与要求

采购包1：2026年业务上云运维服务

通用分册：

详见附件：封面

详见附件：目录

详见附件：投标人（供应商）应提交的相关证明

详见附件：投标人业绩情况表

详见附件：投标人基本情况表

详见附件：具备履行合同所必需设备和专业技术能力的声明函

详见附件：主要商务要求承诺书

详见附件：具有良好的商业信誉和健全的财务会计制度的相关材料

详见附件：技术偏离表

详见附件：具有独立承担民事责任的能力证明文件

详见附件：联合体协议

详见附件：项目实施方案、质量保证及售后服务承诺

详见附件：投标人承诺函

详见附件：依法缴纳税收和社会保障资金的良好记录的相关材料

详见附件：项目组成人员一览表

详见附件：中小企业声明函

详见附件：参加政府采购活动前三年内在经营活动中没有重大违法记录的书面声明

详见附件：缴纳投标保证金证明材料

详见附件：其他材料

详见附件：法定代表人授权委托书

详见附件：监狱企业证明文件

详见附件：残疾人福利性单位声明函

报价分册：

详见附件：分项报价表

详见附件：开标一览表