**信息系统安全等级保护（三级）建设**

**项目**

**招 标 文 件**

**招标人：柘城中医院有限公司**

**日期：2022年03月28日**

[第一章 投标人须知 3](#_Toc73974133)

[投标人须知前附表 3](#_Toc73974134)

[投标人须知正文 7](#_Toc73974135)

[第二章 评标办法（综合评估法） 16](#_Toc73974136)

[评标办法前附表（一） 16](#_Toc73974137)

[评标办法前附表（二） 18](#_Toc73974138)

[第三章 合同条款及格式 23](#_Toc73974139)

[第四章 技术标准和要求 29](#_Toc73974140)

[第五章 投标文件格式 42](#_Toc73974141)

[一、投标函及投标函附录 45](#_Toc73974142)

[（一）投标函 45](#_Toc73974143)

[（二）投标函附录 46](#_Toc73974144)

[二、法定代表人身份证明及授权委托书 47](#_Toc73974145)

[（一）法定代表人身份证明 47](#_Toc73974146)

[（二）授权委托书 48](#_Toc73974147)

[三、已标价建设内容清单 49](#_Toc73974148)

[四、技术参数偏离表 50](#_Toc73974149)

[五、项目设计与实施方案 59](#_Toc73974150)

[六、项目管理机构 61](#_Toc73974151)

[（一）项目管理机构组成表 61](#_Toc73974152)

[（三）主要项目管理人员简历表 64](#_Toc73974153)

[七、资格审查资料 65](#_Toc73974154)

[（一）投标人基本情况表 65](#_Toc73974155)

[（二）近年财务状况表 66](#_Toc73974156)

[（三）近年完成的类似项目情况表 67](#_Toc73974157)

[（四）正在实施的和新承接的项目情况表 68](#_Toc73974158)

[（五）近年发生的诉讼和仲裁情况 69](#_Toc73974159)

[（六）企业其他信誉情况表（年份要求同诉讼及仲裁情况年份要求） 70](#_Toc73974160)

[七、信息系统安等级保护（三级）建设项目招标品牌要求及投标反馈表 73](#_Toc73974161)

[八、项目团队到岗履职承诺书 74](#_Toc73974162)

[九、柘城中医院新冠肺炎疫情防控承诺书 75](#_Toc73974163)

# 第一章 投标人须知

## 投标人须知前附表

|  |  |  |  |
| --- | --- | --- | --- |
| **条款号** | **条 款 名 称** | **编 列 内 容** | |
| 1.1.2 | 招标人 | 柘城中医院有限公司 | |
| 1.1.3 | 招标代理机构 | 无 | |
| 1.1.4 | 项目名称及编号 | 项目名称：柘城中医院信息系统安全等级保护（三级）建设项目 | |
| 1.1.5 | 建设地点 | 商丘市柘城县迎宾大道柘城中医院北关院区 | |
| 1.2.1 | 资金来源及出资比例 | 自筹资金 | |
| 1.2.2 | 资金落实情况 | 已落实 | |
| 1.3.1 | 招标内容及招标范围 | 招标内容：   1. HIS系统信息安全等级保护（三级）测评 2. 信息系统安全等级保护（三级）整改项目设备采购 3. 网络安全服务 | |
| 1.3.2 | 实施周期 | 计划实施周期： 90天  预计实施开始日期：2022年-月-日  预计实施结束日期： 2022年-月-日（按项目签订合同之日起计算项目工期）以取得等保备案证书为准。 | |
| 1.3.3 | 项目目标要求 | 终验一次性验收合格，并取得信息安全等级保护（三级）备案证书。 | |
| 1.4.1 | 投标人资质条件、能力和信誉 | 信息系统安全等级保护（三级）建设项目  （1）资质条件  投标方具备本项目所采购产品厂家有效代理资质、项目授权及售后服务承诺文件，投标方具备本项目下标的物所必需专业技术能力和售后服务能力。  （2）项目管理团队资格：1、投标人配备的项目经理应具备项目管理、网络安全、IT 服务的能力。  （3）服务能力：投标人在惠州市区域内提供自有或租赁的固定场所作为服务场所并为本项目派出人员提供服务，或供应商承诺中标后按上述要求设置服务场所并提供相关服务。  （4）财务要求： 应出具近叁年经会计师事务所或审计部门审计的财务审计报表（2020年-2022年）。投标人的成立时间少于规定年份的，应提供成立以来的财务审计报表，成立不足一年的提供财务状况表。  （5）业绩要求：近三年完成过类似项目。  （6）信誉要求：①拒绝列入政府取消投标资格记录期间的企业或个人投标； ②未被最高人民法院在“信用中国”网站（www.creditchina.gov.cn）列入失信被执行人名单。  （7）履约历史：近三年没有出现违法违规或失信行为，没有骗取中标和严重违约等情况。  （8）其他要求：与招标人存在利害关系可能影响招标公正性的法人、其他组织或个人，不得参加投标。单位负责人为同一人或者存在控股、管理关系的不同单位，不得参加同项目投标。违反这两款规定的，相关投标均无效。 | |
| 1.4.2 | 是否接受联合体投标 | 不接受 | |
| 1.9.1 | 项目调研 | 地 点：柘城中医院信息科  方 式：自行调研 | |
| 1.10.1 | 答疑会 | 不召开 | |
| 1.10.2 | 投标人提出问题的截止时间及方式 | 时 间：2022年 - 月 - 日  投标疑问的提交：邮件形式及书面文本形式  打印后加盖公章，格式见附页，递交原件及发送邮件。时间后所有问题将不再予以答复，其后果投标人自行承担。  送交地点：柘城中医院  联系人：王希 　电话：15637021556  电子邮箱：2833405904@qq.com | |
| 1.10.3 | 招标人书面澄清的时间 | 2022年- 月 -日 | |
| 2.1.1 | 构成招标文件的其他材料 | 无 | |
| 2.2.1 | 投标人要求澄清招标文件的截止时间 | 2022年-月-日 | |
| 2.2.3 | 投标人确认收到招标文件澄清的时间 | 在收到相应澄清文件后 24 小时内 | |
| 2.3.2 | 投标人确认收到招标文件修改的时间 | 在收到相应修改文件后 24 小时内 | |
| 3.1.2 | 构成投标文件的其他材料 | 按招标文件要求的提供证明材料原件   1. 营业执照 2. 开户许可证 3. 资质证书 4. 财务审计报告 5. 类似项目中标通知书和（或）合同   6、招标文件要求的其他材料 | |
| 3.3.1 | 投标有效期 | 30天 | |
| 3.4.1 | 投标保证金 | 无 | |
| 3.5.2 | 近年财务状况的年份要求 | 近三年（2020年-2022年） | |
| 3.5.3 | 近年完成的类似项目的年份要求 | 近三年（2020年-2022年） | |
| 3.5.5 | 近年发生的诉讼及仲裁情况的年份要求 | 近三年（2020年-2022年） | |
| 3.6.3 | 签字或盖章要求 | 按招标文件中提供的格式及要求签字及加盖公章。投标文件中复印件必须加盖公章。副本可以是正本的复印件，加骑缝章。 | |
| 3.6.4 | 投标文件副本份数 | 商务标及技术标，一正贰副，签字盖章电子版（U盘）1份（需包含软件版（word版）的投标报价） | |
| 3.6.5 | 投标文件分册装订 | 投标人可根据投标文件情况可分册装订 | |
| 4.2.2 | 递交投标文件地点 | 地 点：商丘市柘城县迎宾大道柘城中医院北关院区 | |
| 4.2.3 | 是否退还投标文件 | 否 | |
| 5.1 | 开标地点 | 开标地点：柘城中医院有限公司西关院区6楼行政楼中小会议室（要求投标单位到场） | |
| 5.2.1 | 开标程序 | 密封情况检查：评标委员会检查投标文件密封情况；  开标顺序：按投标文件递交顺序进行。 | |
| 6.1.1 | 评标委员会的组建 | 评标委员会构成：共 人 | |
| 7.1 | 是否授权评标委员会确定中标人 | 评标委员推荐中标候选人，由招标方确定最终中标单位 | |
| 10 | 需要补充的其他内容 | | |
| 10.1 | 投标截止时间 | | 2022年-月-日17时00分 |
| 10.2 | 合同付款方式 | | 详见专用合同条款 |
| 10.3 | 投标人的投标代表必须手持法定代表人身份证明文件或法定代表人授权委托书递交投标文件和参加开标会，开标会需对标的项目建设方案向评委进行15分钟介绍，否则不接受投标文件和不允许参加开标会。法定代表人是投标代表的须手持法定代表人身份证明文件，投标代表非法定代表人的须手持法定代表人授权委托书，格式要求详见投标文件格式中相应格式。 | | |
| 10.4 | **答辩和议标时间和地点**  **开标时间：2022年-月-日下午14:30**  地点：柘城中医院有限公司西关院区6楼行政楼中小会议室（要求投标单位到场） | | |
| 10.5 | **采用答辩**  ■是 □否  相关的商务和技术负责人需要于议标日进行现场答辩。  参加答辩和议标的投标人代表要求  1．投标人的法定代表人（或总经理或授权代表人）  2.项目经理、项目合约经理或技术负责人 | | |
| 10.6 | **投标人应理解该项目的目标要求，对标的中涉及的信息系统安全建设内容是否能够达成目标要有明确的判断。** | | |

## 投标人须知正文

**1. 总则**

**1.1 项目概况**

1.1.1根据《中华人民共和国招标投标法》等有关法律、法规和规章的规定，本招标项目已具备招标条件，现对本项目施工进行招标。

1.1.2 本招标项目招标人：见投标人须知前附表。

1.1.3 本招标项目招标代理机构：见投标人须知前附表。

1.1.4 本招标项目名称及编号：见投标人须知前附表。

1.1.5 本招标项目建设地点：见投标人须知前附表。

**1.2 资金来源和落实情况**

1.2.1 本招标项目的资金来源及出资比例：见投标人须知前附表。

1.2.2 本招标项目的资金落实情况：见投标人须知前附表。

**1.3招标内容及招标范围、计划实施周期、项目目标要求**

1.3.1 本次招标内容及招标范围：见投标人须知前附表。

1.3.2 本招标项目的计划实施周期：见投标人须知前附表。

1.3.3 本招标项目的目标要求：见投标人须知前附表。

**1.4 投标人资格要求**

1.4.1 投标人应具备承担本项目施工的资质条件、能力和信誉。

（1）资质条件：见投标人须知前附表；

（2）项目经理资格：见投标人须知前附表；

（3）财务要求：见投标人须知前附表；

（4）业绩要求：见投标人须知前附表；

（5）信誉要求：见投标人须知前附表；

（6）履约历史：见投标人须知前附表；

（7）其他要求：见投标人须知前附表。

1.4.2 投标人须知前附表规定接受联合体投标的，除应符合本章第1.4.1项和投标人须知前附表的要求外，还应遵守以下规定：

（1）联合体各方应按招标文件提供的格式签订联合体协议书，明确联合体牵头人和各方权利义务；

（2）由同一专业的单位组成的联合体，按照资质等级较低的单位确定资质等级；

（3）联合体各方不得再以自己名义单独或参加其他联合体在同一标的中投标。

1.4.3 投标人不得存在下列情形之一：

（1）为招标人不具有独立法人资格的附属机构（单位）；

（2）为本招标项目的监理人；

（3）为本招标项目的代建人；

（4）为本招标项目提供招标代理服务的；

（5）与本招标项目的监理人或代建人或招标代理机构同为一个法定代表人的；

（6）与本招标项目的监理人或代建人或招标代理机构相互控股或参股的；

（7）与本招标项目的监理人或代建人或招标代理机构相互任职或工作的；

（8）被责令停业的；

（9）被暂停或取消投标资格的；

（10）财产被接管或冻结的；

（11）在最近三年内有骗取中标或严重违约或重大工程质量问题的。

1.4.4 单位负责人为同一人或者存在控股、管理关系的不同单位，不得同时参加本招标项目投标。

**1.5 费用承担**

投标人准备和参加投标活动发生的费用自理。

**1.6 保密**

参与招标投标活动的各方应对招标文件和投标文件中的商业和技术等秘密保密，违者应对由此造成的后果承担法律责任。

**1.7 语言文字**

招标投标文件使用的语言文字为中文。专用术语使用外文的，应附有中文注释。

**1.8 计量单位**

所有计量均采用中华人民共和国法定计量单位。

**1.9 项目现场调研**

1.9.1 投标人须知前附表规定组织现场调研的，招标人按投标人须知前附表规定的时间、地点组织投标人项目现场调研。

1.9.2 投标人现场调研过程中发生的费用自理。

1.9.3 除招标人的原因外，投标人自行负责在现场调研中所发生的人员伤亡和财产损失。

1.9.4 招标人在现场调研中介绍的项目概况，供投标人在编制投标文件时参考，招标人不对投标人据此作出的判断和决策负责。

**1.10 答疑会**

1.10.1 不召开答疑会。

1.10.2 投标人应在投标人须知前附表规定的时间前，以书面形式将提出的问题送达招标人，或以邮件形式发送招标人，以便招标人在会议期间澄清。

1.10.3招标人在投标人须知前附表规定的时间内，将对投标人所提问题的澄清，以书面形式或邮件形式通知所有购买招标文件的投标人。该澄清内容为招标文件的组成部分。

**1.11 偏离**

不允许。

**1.12 转包**

不允许。

**2. 招标文件**

**2.1 招标文件的组成**

　　2.1.1 本招标文件包括：

（1）招标公告；

（2）投标人须知；

（3）评标办法；

（4）合同条款及格式；

（5）技术标准和要求；

（6）投标文件格式；

（7）投标人须知前附表规定的其他材料。

2.1.2 根据本章第1.10款、第2.2款和第2.3款对招标文件所作的澄清、修改，构成招标文件的组成部分。

**2.2 招标文件的澄清**

2.2.1 投标人应仔细阅读和检查招标文件的全部内容。如发现缺页或附件不全，应及时向招标人提出，以便补齐。如有疑问，应在投标人须知前附表规定的时间前以书面形式（包括信函、电报、传真等可以有形地表现所载内容的形式，下同），要求招标人对招标文件予以澄清。

2.2.2 招标文件的澄清将以书面形式发给所有购买招标文件的投标人，但不指明澄清问题的来源。如果澄清发出的时间距投标人须知前附表规定的投标截止时间不足7天，并且澄清内容影响投标文件编制的，将相应延长投标截止时间。

2.2.3 投标人在收到澄清后，应在投标人须知前附表规定的时间内以书面形式通知招标人，确认已收到该澄清。

**2.3 招标文件的修改**

2.3.1招标人可以书面形式修改招标文件，并通知所有已购买招标文件的投标人。但如果修改招标文件的时间距投标截止时间不足7天，并且修改内容影响投标文件编制的，将相应延长投标截止时间。

2.3.2 投标人收到修改内容后，应在投标人须知前附表规定的时间内以书面形式通知招标人，确认已收到该修改。

**3. 投标文件**

**3.1 投标文件的组成**

3.1.1投标文件应包括下列内容：

商务标

（1）投标函及投标函附录；

（2）法定代表人身份证明及授权委托书；

（3）已标价项目建设清单；

技术标

（1）项目实施设计

（2）项目管理机构；

（3）资格审查资料；

（4）投标品牌反馈表；

（5）投标人须知前附表规定的其他材料；

3.1.2 构成投标文件的其他材料：见投标人须知前附表。

**3.2 投标报价**

3.2.1 投标人应按第五章“建设项目清单”的要求填写相应表格。

3.2.2 投标人在投标截止时间前修改投标函中的投标报价总额，应同时修改“建设项目清单”中的相应报价，投标报价总额为各分项金额之和。此修改须符合本章第4.3款的有关要求。

3.2.3 招标人设有最高投标限价的，投标人的投标报价不得超过最高投标限价，最高投标限价或其计算方法在投标人须知前附表中载明。

**3.3 投标有效期**

3.3.1 除投标人须知前附表另有规定外，投标有效期为30天。

3.3.2在投标有效期内，投标人撤销或修改其投标文件的，应承担招标文件和法律规定的责任。

3.3.3出现特殊情况需要延长投标有效期的，招标人以书面形式通知所有投标人延长投标有效期。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（如有）。

**3.4 投标保证金（如有）**

3.4.1 投标人须知前附表规定递交投标保证金的，投标人在递交投标文件的同时，应按投标人须知前附表规定的金额、形式和第八章“投标文件格式”规定的或者事先经过招标人认可的投标保证金格式递交投标保证金，并作为其投标文件的组成部分。

3.4.2 投标人不按本章第3.4.1项要求提交投标保证金的，评标委员会将否决其投标。

3.4.3 投标保证金的退还

3.4.3.1 未中标投标单位的投标保证金，除因处理异议、投诉等原因外，在中标公示期结束后五日内返还。

3.4.3.2 中标人的投标保证金应在签订合同后五日内返还。

3.4.3.3 未中标投标单位的投标保函原件在中标公示期结束后五日内返还，中标人的投标保函原件在签订合同后五日内返还。

3.4.4 有下列情形之一的，投标保证金将不予退还：

（1）投标人未参加投标。

（2）投标人在规定的投标有效期内撤销或修改其投标文件；

（3）中标人在收到中标通知书后，无正当理由拒签合同协议书。

**3.5 资格审查资料**

3.5.1 “投标人基本情况表”应附投标人营业执照及其年检合格的证明材料、资质证书副本的复印件等材料的复印件。

3.5.2 “近年财务状况表”应附经会计师事务所审计的财务会计报表，包括资产负债表、现金流量表、利润表和财务情况说明书等复印件，具体年份要求见投标人须知前附表。

3.5.3 “近年完成的类似项目情况表”应附中标通知书或合同协议书、项目验收文件或项目最终完成备案等保备案证书复印件，具体年份要求见投标人须知前附表。每张表格只填写一个项目，并标明序号。

3.5.4 “正在实施和新承接的项目情况表”应附中标通知书或合同协议书复印件。每张表格只填写一个项目，并标明序号。

3.5.5 “近年发生的诉讼及仲裁情况”应说明相关情况，并附法院或仲裁机构作出的判决、裁决等有关法律文书复印件，具体年份要求见投标人须知前附表。

**3.6投标文件的编制**

3.6.1投标文件应按第八章“投标文件格式”进行编写，如有必要，可以增加附页，作为投标文件的组成部分。其中，投标函附录在满足招标文件实质性要求的基础上，可以提出比招标文件要求更有利于招标人的承诺。

3.6.2 投标文件应当对招标文件有关实施周期、投标有效期、质量要求、技术标准和要求、招标范围等实质性内容作出响应。

3.6.3投标文件应用不褪色的材料书写或打印，并由投标人的法定代表人或其委托代理人签字或盖单位章。委托代理人签字的，投标文件应附法定代表人签署的授权委托书。投标文件应尽量避免涂改、行间插字或删除。如果出现上述情况，改动之处应加盖单位章或由投标人的法定代表人或其授权的代理人签字确认。签字或盖章的具体要求见投标人须知前附表。

3.6.4 投标文件正本一份, 副本份数见投标人须知前附表。正本和副本的封面上应清楚地标记“正本”或“副本”的字样。当副本和正本不一致时，以正本为准。

3.6.5 投标文件的正本与副本应分别装订成册，具体装订要求见投标人须知前附表规定。

**3.7 备选投标方案**

不接受

**4. 投标**

**4.1 投标文件的密封和标记**

4.1.1 投标文件应进行包装、加贴封条，并在封套的封口处加盖投标人单位章。

4.1.2 投标文件封套上应写明 “柘城中医院信息安全等级保护（三级）建设项目– 投标文件（密件）”

4.1.3 未按本章第4.1.1项或第4.1.2项要求密封和加写标记的投标文件，招标人应予拒收。

**4.2 投标文件的递交**

4.2.1 投标人应在本章第10.1项规定的投标截止时间前递交投标文件。

4.2.2 投标人递交投标文件的地点：见投标人须知前附表。

4.2.3 除投标人须知前附表另有规定外，投标人所递交的投标文件不予退还。

4.2.4 招标人收到投标文件后，向投标人出具签收凭证。

4.2.5 逾期送达的或者未送达指定地点的投标文件，招标人不予受理。

**4.3 投标文件的修改与撤回**

4.3.1 在本章第10.1项规定的投标截止时间前，投标人可以修改或撤回已递交的投标文件，但应以书面形式通知招标人。

4.3.2 投标人修改或撤回已递交投标文件的书面通知应按照本章第3.6.3项的要求签字或盖章。招标人收到书面通知后，向投标人出具签收凭证。

4.3.3 投标人撤回投标文件的，招标人自收到投标人书面撤回通知之日起5日内退还已收取的投标保证金（如有）。

4.3.4 修改的内容为投标文件的组成部分。修改的投标文件应按照本章第3条、第4条规定进行编制、密封、标记和递交，并标明“修改”字样。

**5. 开标**

**5.1 开标时间和地点**

招标人在本章第10.1项规定的投标截止时间（开标时间）和投标人须知前附表规定的地点公开开标。

**6. 评标**

**6.1 评标委员会**

6.1.1 评标由招标人依法组建的评标委员会负责。评标委员会由招标人或其委托的招标代理机构熟悉相关业务的代表，以及有关技术、经济等方面的专家组成。评标委员会成员人数以及技术、经济等方面专家的确定方式见投标人须知前附表。

6.1.2 评标委员会成员有下列情形之一的，应当回避：

（1）投标人或投标人主要负责人的近亲属；

（2）项目主管部门或者行政监督部门的人员；

（3）与投标人有经济利益关系；

（4）曾因在招标、评标以及其他与招标投标有关活动中从事违法行为而受过行政处罚或刑事处罚的；

（5）与投标人有其他利害关系。

**6.2 评标原则**

评标活动遵循公平、公正、科学和择优的原则。

**6.3 评标**

评标委员会按照第三章“评标办法”规定的方法、评审因素、标准和程序对投标文件进行评审。第三章“评标办法”没有规定的方法、评审因素和标准，不作为评标依据。

**7. 合同授予**

**7.1 定标方式**

招标人依据评标委员会推荐的中标候选人确定中标人。

**7.2 中标通知**

在本章第3.3款规定的投标有效期内，招标人以书面形式向中标人发出中标通知书，同时将中标结果通知未中标的投标人。

**7.3 签订合同**

7.3.1招标人和中标人应当自中标通知书发出之日起30天内，根据招标文件和中标人的投标文件订立书面合同。给招标人造成的损失中标人还应当予以赔偿。

7.3.2 发出中标通知书后，招标人无正当理由拒签合同的；给中标人造成损失的，还应当赔偿损失。

**8．重新招标和不再招标**

**8.1 重新招标**

有下列情形之一的，招标人将重新招标：

(l）投标截止时间止，投标人少于3 个的；

(2）经评标委员会评审后否决所有投标的。

**8.2 不再招标**

重新招标后投标人仍少于3 个或者所有投标被否决的，招标人有权可不再进行招标。

**9. 纪律和监督**

**9.1 对招标人的纪律要求**

招标人不得泄漏招标投标活动中应当保密的情况和资料，不得与投标人串通损害国家利益、社会公共利益或者他人合法权益。

**9.2 对投标人的纪律要求**

投标人不得相互串通投标或者与招标人串通投标，不得向招标人或者评标委员会成员行贿谋取中标，不得以他人名义投标或者以其他方式弄虚作假骗取中标；投标人不得以任何方式干扰、影响评标工作。

**9.3 对评标委员会成员的纪律要求**

评标委员会成员不得收受他人的财物或者其他好处，不得向他人透漏对投标文件的评审和比较、中标候选人的推荐情况以及评标有关的其他情况。在评标活动中，评标委员会成员应当客观、公正地履行职责，遵守职业道德，不得擅离职守，影响评标程序正常进行，不得使用第三章“评标办法”没有规定的评审因素和标准进行评标。

**9.4 对与评标活动有关的工作人员的纪律要求**

与评标活动有关的工作人员不得收受他人的财物或者其他好处，不得向他人透漏对投标文件的评审和比较、中标候选人的推荐情况以及评标有关的其他情况。在评标活动中，与评标活动有关的工作人员不得擅离职守，影响评标程序正常进行。

**10. 需要补充的其他内容**

需要补充的其他内容：见投标人须知前附表。

**第二章 评标办法（综合评估法）**

## 评标办法前附表（一）

|  |  |  |  |
| --- | --- | --- | --- |
| **条款号** | | **评审因素** | **评审标准** |
| 2.1.1 | 形式  评审  标准 | 投标人名称 | 与营业执照、资质证书一致 |
| 投标函签字盖章 | 有法定代表人或其委托代理人签字或加盖单位章 |
| 投标文件格式 | 符合第五章“投标文件格式”的要求 |
| 报价唯一 | 只能有一个有效报价 |
| 2.1.2 | 资格  评审  标准 | 营业执照 | 具备有效的营业执照 |
| 企业资质 | 投标方具备本项目所采购产品厂家有效代理资质、项目授权及售后服务承诺文件，投标方具备本项目下标的物所必需专业技术能力和售后服务能力。  （投标人需提供相关材料证明文件，原件备查。） |
| 企业业绩 | 近三年完成过类似项目业绩 |
| 项目经理 | 1、须具备建信息系统安全等级保护建设项目经验，具备有效的网络工程师认证（中级及以上）或信息安全等级保护2.0认证相关证书，并提供近六个月社保证明。 |
| 财务要求 | 应出具近三年（2020年-2022年）每一年经会计师事务所或审计部门审计的财务审计报告。投标人的成立时间少于规定年份的，应提供成立以来的财务审计报表，成立不足一年的提供财务状况表。 |
| 信誉要求 | 拒绝列入政府取消投标资格记录期间的企业或个人投标。投标人须提供法人代表或其授权委托人签字或加盖公章的承诺书。 |
| 信誉要求  履约历史 | 未被最高人民法院在“信用中国”网站（www.creditchina.gov.cn）列入失信被执行人名单。  标书内附“信用中国”网站查询结果截图加盖投标单位公章 |
| 近三年（2018年-2020年）没有出现违法违规或失信行为，没有骗取中标和严重违约及重大工程质量事故，投标人须提供法人代表或其授权委托人签字或加盖公章的承诺书。 |
| 授权委托书  （如有委托代理人） | 有法定代表人及委托代理人签字并加盖公章 |
| 不存在禁止投标情形 | 不存在第一章“投标人须知”的任何一种情形。 |
| 投标报价 | 投标报价不得超过招标控制价 |
| 2.1.3 | 响应性  评审  标准 | 投标内容 | 符合投标人须知前附表要求 |
| 计划实施开始日期 | 符合投标人须知前附表要求 |
| 项目目标要求 | 终验一次性验收合格，并取得信息安全等级保护（三级）备案证书。 |
| 投标有效期 | 30天 |
| 投标保证金 | 符合投标人须知前附表要求 |
| 权利义务 | 符合第三章“合同条款及格式”规定 |
| 已标价项目建设清单 | 应按招标人提供的项目建设清单填报价格。填写的项目编号、项目名称、规格参数、数量应与招标人提供的一致。 |
| 技术标准和要求 | 符合第四章“技术标准和要求”规定 |

只对经过评审确定有效标书的投标文件进入评审，本项目使用综合评标办法进行评标。

## 评标办法前附表（二）

|  |  |  |  |
| --- | --- | --- | --- |
| **条款号** | | **条款内容** | **编列内容** |
| 2.2.1 | | 分值构成  (总分100分) | 商务部分： 20 \_分  技术部分： 20 分  投标报价： 60\_\_分 |
| 2.2.2 | | 评标基准价计算方法 | 经初步评审合格的有效投标大于等于5家，投标报价的算术平均值下浮5%作为评标基准价；经初步评审合格的有效报价小于5家，取投标报价的算术平均值作为评标基准价。 |
| 2.2.3 | | 投标报价的偏差率计算公式 | 偏差率=100% ×（投标人报价−评标基准价）/评标基准价 |
| **条款号** | | **评分因素** | **评分标准** |
| 2.2.4（1） | 商务部份评分标准20分 | 企业资质（6分）  （投标人需提供相关材料证明文件，原件备查。） | 1. 投标人同时具有有效的IS09001 质量体系认证、“守合同重信用”证书。（满分2分） |
| 2. 投标人同时具有有效的计算机信息系统集成资质或信息系统建设和服务能力评估CS1认证及ITSS运维评估认证。（满分2分） |
| 3. 投标人同时具有有效的计算机信息系统安全服务等级证、信息系统安全服务资质CCRC认证及信息安全管理体系ISO27001认证。（满分2分） |
| 服务能力（5分） | 投标人配备的项目经理应具备项目管理、网络安全、IT服务的能力，在同时具有中级及以上网络工程师认证（1分）、IT服务项目经理认证或IT服务工程师认证（1分）、信息安全等保2.0认证（1分）。（满分3分） |
| 投标人配备的2名项目组成员，每成员同时具有信息安全等保2.0 认证和网络工程师认证（中级）（每人1分，满分2分）。 |
| 企业业绩（3分） | 近三年完成过类似项目业绩（信息安全等保整改项目，项目金额在80万元以上，并取得等级保（三级）验收的项目）；（每个项目1分，满分3分）。 |
| 财务要求（2分） | 应出具近三年（2020年-2022年）每一年经会计师事务所或审计部门审计的财务审计报告。投标人的成立时间少于规定年份的，应提供成立以来的财务审计报表，成立不足一年的提供财务状况表。（提供一年审计报告得0.5分，没有不得分，满分2分） |
| 信誉要求（1分） | 拒绝列入政府取消投标资格记录期间的企业或个人投标。投标人须提供法人代表或其授权委托人签字或加盖公章的承诺书。未被最高人民法院在“信用中国”网站（www.creditchina.gov.cn）列入失信被执行人名单标书内附“信用中国”网站查询结果截图加盖投标单位公章。（满分1分） |
| 履约历史（1分） | 近三年（2020年-2022年）没有出现违法违规或失信行为，没有骗取中标和严重违约及重大工程质量事故，投标人须提供法人代表或其授权委托人签字或加盖公章的承诺书。（满分1分） |
| 项目实施周期承诺（2分） | 按标的要求90天取得备案证书，承诺小于60天，得2分；承诺90天得1分，否则0分。（满分2分） |
| 2.2.4（2） | 技术部分评分标准  20分 | 设备技术参数响应程度（8分） | 投标设备参数符合招标文件中设备参数要求，完全响应无负向偏离得4分。（技术参数标“▲”的重要指标，一个负偏离减2分；其他指标负向偏离，每项目扣0.5分，扣分不设下限），相关技术标准有截图证明的可酌情加分。（满分8分） |
| 投标设备技术参数项需按招标文件中设备清单的备注的要求提供证明材料，没按要求提供证明材料的，该大项不得分。  说明材料包括：a.原厂商针对本项目盖章确认的产品授权函；或 b.原厂商官方网站的技术白皮书打印稿加盖原厂商公章确认，同时注明材料来源于官方网站的网址。 |
| 设备品牌响应（4分） | 投标设备符合招标文件品牌响应表要求，（选择非推荐品牌，请按招标品牌要求及投标反馈表备注第2项要求提供资料，否则每偏离一项扣1分）。（满分4分） |
| 售后服务（6分） | 投标设备（含设备的相关软件升级服务）满足3年保修期得3分，否则0分。（满分3分） |
| 本次招标项目所涉及的网络安全服务等服务期限至少1年，服务方案优得3分，一般得1分，无不得分。（满分3分） |
| 项目实施方案与实施计划安排（2分） | 根据投标人针对本项目建设详细调研，能够提出详细、合理的总体设计方案进行综合评比：  提供项目总体网络安全架构，详细描述本项目详细规划，提供网络拓扑图，提供信息安全架构设计方案，合理布局，提供系统拓扑图，提供项目的具体实施方案与项目组织架构及详细实施周期计划安排表（横道图），根据方案合理设计详细程度评分，优得2分，一般得1分，无提供不得分；（满分2分） |
| 2.2.4（3） | 投标报价评分标准  60分 | 偏差率 | 以2.2.3确定的公式计算 |
| 评分标准 | 当偏差率<0时，报价得分=40+︱偏差率︱\*200（上限60分）  当偏差率=0时，报价得分=40  当偏差率>0时，报价得分=40-︱偏差率︱×200(最低分0) |

评标办法正文

**1. 评标方法**

本次评标采用综合评估法。评标委员会对所有的投标文件进行形式、资格及响应性文件评审，并经答辩、议标及最终优惠让利报价后，按照本章第2.2款规定的评分标准进行打分，对各项评分进行汇总，将所有评委的打分进行汇总后，所有评委的算术平均值为投标单位的最后得分，并将得分由高到低顺序推荐三名中标候选人，由招标人最终确定中标人。

**2. 评审标准**

**2.1 初步评审标准**

2.1.1 形式评审标准：见评标办法前附表。

2.1.2 资格评审标准：见评标办法前附表。

2.1.3 响应性评审标准：见评标办法前附表。

**2.2 分值构成与评分标准：**见评标办法前附表

**3. 评标程序**

**3.1 投标文件符合性鉴定：**

3.1.1开标后，投标文件经招标人按初步评审标准审查符合规定的投标文件才能提交招标人进行评标

3.1.2招标人会将首先判定每份投标文件是否在实质上响应了招标文件的要求，所谓实质上响应，是指投标文件应与招标文件的所有实质性条款、条件和要求相符，无显著差异和保留，纠正这些显著差异或保留将不会对其他实质上响应招标文件要求的投标文件的投标人的竞争地位产生不公正的影响

3.1.3只有通过初步评审的的投标人才能够进入后续详细评审。

**3.2 详细评审**

3.2.1 投标人需对该项目进行15分钟左右项目实施方案计划进行介绍，评标委员会按本章第2.2款规定的评审因素和分值进行打分，并计算出综合评估得分。

3.2.2 评标委员会发现投标人的报价明显低于其他投标报价，或者在设有标底时明显低于标底，使得其投标报价可能低于其个别成本的，应当要求该投标人作出书面说明并提供相应的证明材料。投标人不能合理说明或者不能提供相应证明材料的，评标委员会应当认定该投标人以低于成本报价竞标，否决其投标。

3.2.3评标委员会审查投标文件，审核并确认清标结果，包括工程投标报价的校核、审核全部数据计算的正确性、分析各种费用构成的合理性和正确性等内容，看其是否有计算或表达上的错误，投标报价有算术错误的，评标委员会按以下原则对投标报价进行修正：

① 投标文件中的大写金额与小写金额不一致的，以大写金额为准；

② 总价金额与依据单价计算出的结果不一致的，以单价金额为准修正总价，但单价金额小数点有明显错误的除外。

**3.3 投标文件的澄清和补正**

3.3.1在评标过程中，评标委员会可以书面形式要求投标人对所提交投标文件中不明确的内容进行书面澄清或说明，或者对细微偏差进行补正。评标委员会不接受投标人主动提出的澄清、说明或补正。

3.3.2 澄清、说明和补正不得改变投标文件的实质性内容，但是招标人在评标中发现的计算错误并进行核实的修改不在此列。投标人的书面澄清、说明和补正属于投标文件的组成部分。

3.3.3 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，直至满足评标委员会的要求。

**3.4 评标结果**

3.4.1评标委员会按投标人的综合得分由高到低的顺序推荐三名中标候选人，由招标人确定最终中标人。若中标候选人放弃中标、因不可抗力提出不能履行合同、或者被查实存在影响中标结果的违法行为等情形，不符合中标条件的，招标人可以按照评标委员会提出的中标候选人名单排序依次确定其他中标候选人为中标人，也可以重新招标。

3.4.2 评标委员会完成评标后，应当向招标人提交书面评标报告。

# 第三章 合同条款及格式

**柘城中医院有限公司**

**信息安全等级保护（三级）建以项目采购**

**合 同 书**

|  |
| --- |
| **合同编号：** |
|  |
|  |
|  |

**注：本合同仅为合同的参考文本，合同签订双方可根据项目的具体要求进行修订。**

**甲 方：**

电 话： 传 真： 地 址：

**乙 方：**电 话： 传 真： 地 址：

项目名称：柘城中医院有限公司信息系统安全等级保护（三级）建设项目

根据 柘城中医院有限公司信息系统安全等级保护（三级）建设项目的采购结果，按照《合同法》的相关要求，经双方协商，本着平等互利和诚实信用的原则，一致同意签订本合同如下。

**一、采购项目内容**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 序号 | 商品名称 | 品牌、规格型号、配置（性能参数） | 产地 | 数量 | 单价（元） | 合计(元) | 备注 |
| 1 |  |  |  |  |  |  |  |
| 2 |  |  |  |  |  |  |  |
| 3 |  |  |  |  |  |  |  |
| 4 |  |  |  |  |  |  |  |
| 合同总额：￥ 元；大写： | | | | | | | |

合同总额包括乙方设计、安装、随机零配件、标配工具、运输保险、调试、培训、质保期服务、各项税费及合同实施过程中不可预见费用等。

注：采购项目名称内容必须与投标文件中项目名称内容一致。

**二、合同金额**

合同总额为（大写）： 元（￥ 元）人民币。

**三、设备要求**

1、本项目采购设备为原制造商制造的全新产品，整机无污染，无侵权行为、表面无划损、无任何缺陷隐患，在中国境内可依常规安全合法使用。

2、交付验收标准依次序对照适用标准为：①符合中华人民共和国国家安全质量标准、环保标准或行业标准；②符合采购文件和响应承诺中甲方认可的合理最佳配置、参数及各项要求；③货物来源国官方标准。

4、货物为原厂商未启封全新包装，具出厂合格证，序列号、包装箱号与出厂批号一致，并可追索查阅。

5、乙方应将关键主机设备的用户手册、保修手册、有关单证资料及配备件、随机工具等交付给甲方，使用操作及安全须知等重要资料应附有中文说明。

**四、完工时间、交货方式及交货地点**

1. **完工时间：**签订合同后30天内交货、安装调试完成并交付使用。
2. **交货方式： \_\_\_\_\_\_\_\_\_\_\_。**
3. **交货地点：**用户指定地点。

**五、付款方式：**

（1）双方签订合同后，甲方向乙方支付合同总金额的30%作为预付款。

（2）乙方所有硬件设备到货初验合格后即进行项目安装调试，经验收合格后，甲方向乙方支付合同总金额的40%。

（3）待项目达到本次项目建设目标时，即取得信息系统安全等级保护（三级）备案证书后，支付合同金额尾款30%。

**六、质保期及售后服务要求：**

1、保修期限：乙方所投设备必须满足用户需求中提出的质保期要求，未有具体要求的，按厂家标准（其中设备保修期为3年，按验收之日起计），若厂商标准超过3年的，则按厂商标准执行。

2、保修期内，乙方负责对其提供的设备整体进行维修和系统维护，不再收取任何费用，但人为因素，自然因素（如火灾、地震等）造成的故障除外。

3、保修期内乙方所投设备各部件发生非人为故障，乙方应免费上门更换同种品牌不低于原规格型号的新部件。

4、保修期间内同一硬件一个月内连续3次出现同一故障，乙方须无偿更换同一档次设备。

5、保修期后，产品厂商须继续提供产品使用运行的技术支持，包括故障排除及零备件的供应等。

6、提供所投设备售后维修电话及联系人，系统故障保修响应时间为：周一至周日8：30―18：00期间15分钟内电话响应，1小时内到现场响应。其余期间为2小时内到现场响应。用户报修后须在上述规定的时间内派人员上门现场维护，并在12小时内解决问题。在12小时内不能解决问题的设备，应提供不低于故障产品档次的设备给用户使用，直至故障设备修复。

**七、安装与调试:** 乙方负责合同项下设备的运输、安装及调试，一切费用由乙方负责。乙方安装时必须对各安装场地内的其它设备、设施有良好保护措施。

**八、验收：**

1、验收要求：

1) 设备安装调试完成正常工作的7个工作日内，验收应在甲方和乙方双方共同参加下进行。

2) 验收按国家有关的规定、规范进行。

3) 验收时如发现所交付的设备有短装、次品、损坏或其它不符合招标文件规定之情形者，甲方应做出详尽的现场记录，或由甲方和乙方双方签署备忘录。此现场记录或备忘录可用作补充、缺失和更换损坏部件的有效证据。由此产生的有关费用由乙方承担。

4) 培训：为了使用户指定的员工能熟练操作设备系统，保证设备系统良好运作，乙方应提供免费培训服务计划，按甲方要求培训2名操作管理及维护人员，达到熟练掌握产品性能和能及时排除一般故障的程度。

**九、违约责任与赔偿损失**

1) 乙方交付的设备、提供的服务不符合采购文件、报价文件或本合同规定的，甲方有权拒收，并且乙方须向甲方支付本合同总价5%的违约金。

2) 乙方未能按本合同规定的交货时间交付设备的/提供服务，从逾期之日起每日按本合同总价3‰的数额向甲方支付违约金；逾期半个月以上的，甲方有权终止合同，由此造成的甲方经济损失由乙方承担。

3) 甲方无正当理由拒收设备/接受服务，到期拒付设备/服务款项的，甲方向乙方偿付本合同总的5%的违约金。甲方人逾期付款，则每日按本合同总价的3‰向乙方偿付违约金。

4）乙方承诺甲方在\_\_\_\_天内完成项目实施，即取得HIS系统三级等保备案证书，若有延期，则每日按本合同总价的3‰向乙方偿付违约金。

5) 其它违约责任按《中华人民共和国合同法》处理。

**十、争议的解决**

1)合同执行过程中发生的任何争议，如双方不能通过友好协商解决，按相关法律法规处理。

**十一、不可抗力：**任何一方由于不可抗力原因不能履行合同时，应在不可抗力事件结束后1日内向对方通报，以减轻可能给对方造成的损失，在取得有关机构的不可抗力证明或双方谅解确认后，允许延期履行或修订合同，并根据情况可部分或全部免于承担违约责任。

**十二、税费：**在中国境内、外发生的与本合同执行有关的一切税费均由乙方负担。

**十三、其它**

1) 本合同所有附件、采购文件、投标文件、中标通知书通知书均为合同的有效组成部分，与本合同具有同等法律效力。

2) 在执行本合同的过程中，所有经双方签署确认的文件（包括会议纪要、补充协议、往来信函）即成为本合同的有效组成部分。

3) 如一方地址、电话、传真号码有变更，应在变更当日内书面通知对方，否则，应承担相应责任。

4) 除甲方事先书面同意外，乙方不得部分或全部转让其应履行的合同项下的义务。

**十四、合同生效：**

1）本合同在甲乙双方法人代表或其授权代表签字盖章后生效。

2）合同一式 3 份。

**甲方（盖章）： 乙方（盖章）：**

**代表： 代表：**

签定地点：

签定日期： 年 月 日 签定日期： 年 月 日

开户名称：

银行帐号：

开 户 行：

# 第四章 技术标准和要求

1项目概述

信息安全形势严峻，国家陆续颁布了网络和信息安全方面新的法律法规和政策文件，提出更高的工作标准，保持对信息安全保护工作的高度要求。信息系统承担着越来越重要的支撑角色，信息安全已成为医院医疗工作的重要组成部分，关系医院的运营，影响百姓民生。2017年6月1日起《中华人民共和国网络安全法》正式施行，对信息各范畴信息安全提出权威性要求，确定信息安全的法定地位；2018年以来，国家在更新原有法律法规和标准规范的同时，出台了多类网络和信息安全新的法律法规和政策文件，包括《信息安全技术个人信息安全规范》（2018年5月1日正式实施）、《网络安全等级保护条例（征求意见稿）》（2018年6月27日）、《互联网个人信息安全保护指引（征求意见稿）》（2018年11月30日）等，以及2019年即将实施的信息系统等级保护2.0标准，对医院和公民信息安全提出更高的标准要求。

以“保障应用、确保安全”为目标，按照统筹规划、同步建设，分级管理、逐级负责，属地管理、明确责任的原则，依据国家网络安全等级保护三级标准要求，建立和完善医院通信网络安全保障系统，增强精确感知的安全预警能力、及时有效的安全防御能力、快速响应的应急处置和安全可靠的灾难恢复能力，实现网络安全由边界防护、被动防御向全域联动、主动防御转变，提高医院通信网络整体防护水平。最终协助测评机构通过网络安全等级保护最终测评验收，获取备案证书。

2建设依据

（1）《中华人民共和国网络安全法》（2017年6月1日）

（2）《网络安全等级保护管理条例》（征求意见稿）

（3）《网络安全等级保护定级指南》（GB/T 22240-2020）

（4）《网络安全等级保护基本要求》（GB/T 22239-2019）

（5）《网络安全等级保护安全设计技术要求》（GB/T 25070-2019）

（6）《网络安全等级保护实施指南》（GB/T 25058-2019）

（7）《信息安全风险评估规范》（GB/T 20984-2007）

（8）卫生部关于印发《卫生行业信息安全等级保护工作的指导意见》的通知

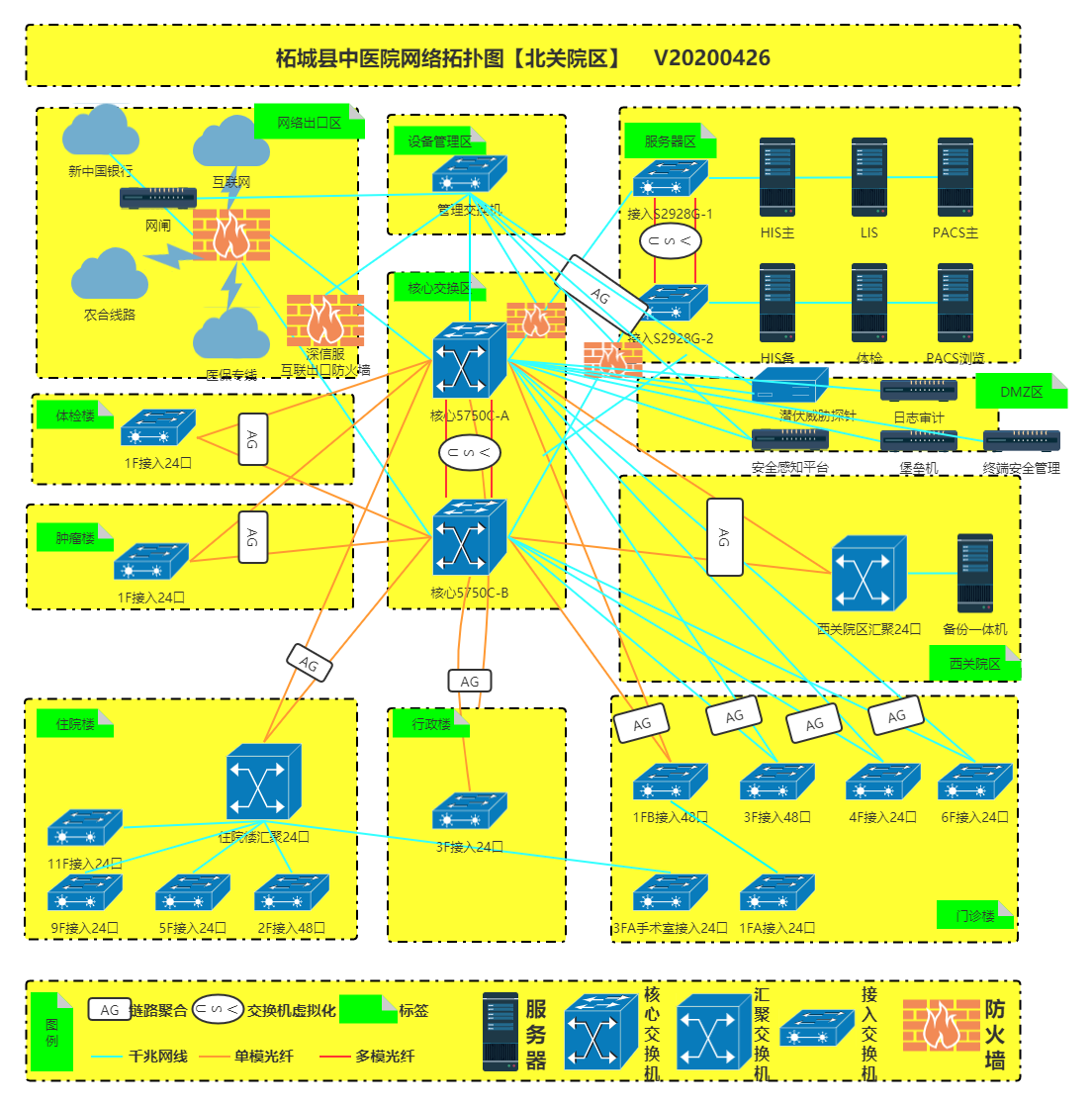
3 项目现况

3.1 机房物理环境

柘城中医院的物理机房有静电地板、视频监控系统、烟雾探测系统、温湿度监测系统、气体消防系统、UPS供电系统、精密空调、门禁系统、动环监测系统等满足等级保护三级的机房物理设施类要求，需要稍加补全制度、流程、规范即满足安全物理环境要求。

3.2网络安全技术

目前医院网络架构具备深信服边界防火墙、深信服数据中心防火墙，网络互联互通和互联网边界安全基本满足安全区域边界要求，但是对于安全计算环境、安全管理中心、业务系统的安全区域边界基本不满足、内外网未作物理隔离等，需要对业务系统的边界区域划分隔离、全网威胁检测、数据库的操作审计记录、运维的统一管理审计和全网日志保存180天等相关要求进行加固建设，使满足等级保护要求。网络现状架构图如下图所示：



4 网络安全等级保护需求

4.1 物理环境安全需求

物理环境安全主要影响因素包括机房环境、机柜、电源、通信线缆和其他设备的物理环境。该层面为基础设施和业务应用系统提供了一个生成、处理、存储和传输数据的物理环境。具体安全需求如下：

（1）由于机房容易遭受雷击、地震和台风和暴雨等自然灾难威胁，需要考虑机房场地位置的选择，以及采取防雷击措施等来解决雷击、地震和台风等威胁带来的问题；

（2）由于机房容易遭受水患和火灾等灾害威胁，需要采取防水、防潮、防火措施来解决水患和火灾等威胁带来的安全威胁；

（3）由于机房容易遭受高温、低温、多雨等原因引起温度、湿度异常，应采取温湿度控制措施来解决因高温、低温和多雨带来的安全威胁；

由于机房电压波动影响，需要合理设计电力供应系统来解决因电压波动带来的安全威胁；

（4）针对机房供电系统故障，需要合理设计电力供应系统，如：购买UPS系统、建立发电机机房，铺设双电力供电电缆来保障电力的供应，来解决因供电系统故障带来的安全威胁；

（5）针对机房容易遭受静电和线缆电磁干扰，需要采取防静电和电磁防护措施来解决静电和线缆电磁干扰带来的安全威胁；并对关键设备采取电磁屏蔽措施；

（6）针对利用非法手段进入机房内部盗窃、破坏等安全威胁，需要通过采取物理访问控制及监控报警装置等控制措施，来解决非法手段进入机房内部盗窃、破坏等带来的安全问题；

（6）针对利用工具捕捉电磁泄漏的信号，导致信息泄露的安全威胁，需要通过采取防电磁措施，来解决电磁泄漏带来的安全问题。

4.2 通信网络安全需求

通信网络是对定级系统安全计算环境之间进行信息传输及实施安全策略的安全部件。是利用网络设备、安全设备、服务器、通信线路以及接入链路等设备或部件共同建成的、可以用于在本地或远程传输数据的网络环境。具体安全需求如下：

（1）针对网络架构设计不合理而影响业务通信或传输问题，需要通过优化网络设计、改造网络安全域来完成。

（2）针对线路或设备的单点故障问题，需要采取冗余设计来确保系统的可用性。

（3）针对利用通用安全协议、算法、软件等缺陷获取信息或破坏通信完整性和保密性，需要通过数据加密技术、数据校验技术来保障。

（4）针对通过伪造信息进行应用系统数据的窃取风险，需要加强网络边界完整性检查，加强对网络设备进行防护、对访问网络的用户身份进行鉴别，加强数据保密性来解决。

（5）针对病毒入侵、恶意代码加载、非授权身份访问等安全威胁，通信设备需要通过采取动态可信验证机制来确保程序运行安全可信，从而保障业务系统安全可信。

4.3区域边界安全需求

区域边界包括安全计算环境边界，以及安全计算环境与安全通信网络之间实现连接并实施安全策略的相关部件，区域边界安全即各网络安全域边界和网络关键节点可能存在的安全风险。需要把可能的安全风险控制在相对独立的区域内，避免安全风险的大规模扩散。

各类网络设备、服务器、管理终端和其他办公设备系统层的安全风险。主要涵盖两个方面，一是来自系统本身的脆弱性风险；另一个是来自用户登录帐号、权限等系统使用、配置和管理等风险。具体如下：

（1）针对内部人员未授权违规连接外部网络，或者外部人员未经许可随意接入内部网络而引发的安全风险，以及因使用无线网络传输的移动终端而带来的安全接入风险等问题，需要通过违规外联、安全准入控制以及无线安全控制措施来解决。

（2）针对跨安全域访问网络的行为，需要通过基于应用协议和应用内容的细粒度安全访问控制措施来解决，以实现网络访问行为可控可管。

（3）针对通过分布式拒绝服务攻击恶意地消耗网络、操作系统和应用系统资源，导致拒绝服务或服务停止的安全风险，需要通过抗DDoS攻击防护、服务器主机资源优化、入侵检测与防范、网络结构调整与优化等手段来解决。

（4）针对利用网络协议、操作系统或应用系统存在的漏洞进行恶意攻击（如碎片重组，协议端口重定位等），需通过网络入侵检测和防范等技术措施来解决。

（5）针对通过恶意代码传播对主机、应用系统和个人隐私带来的安全威胁，需要通过恶意代码防护技术手段解决。

（6）针对邮件收发时遭受恶意代码攻击的安全风险，，需要通过垃圾邮件防护等技术手段解决。

（7）针对违规越权操作、违规访问网络等用户行为，需要采取安全审计手段来实现安全事件的有效追溯和用户行为的审计分析。

（8）针对病毒入侵、恶意代码加载、非授权身份访问等安全威胁，边界设备需要通过采取动态可信验证机制来确保程序运行安全可信，从而保障业务系统安全可信。

4.4 计算环境安全需求

计算环境安全涉及业务应用系统及重要数据处理、存储的安全问题。具体安全需求如下：

（1）针对用户帐号权限设置不合理、帐号暴力破解等等安全风险，需要通过帐号管理、身份鉴别、访问控制等技术手段解决。

（2）针对在网页浏览、文档传递、介质拷贝或文件下载、邮件收发时而遭受恶意代码攻击的安全风险，需通过恶意代码防范、入侵防范等技术手段解决。

（3）针对操作用户对系统错误配置或更改而引起的安全风险，需通过安全配置核查、终端安全管控等技术手段解决。

（4）针对设备系统自身安全漏洞而引起被攻击利用的安全风险，需要通过漏洞扫描技术、安全加固服务等手段解决。

（5）针对攻击者越权访问文件、数据或其他资源，需要通过访问控制、身份鉴别、安全审计等技术来解决。

（6）针对利用各种工具获取应用系统身份鉴别数据，进行分析获得鉴别内容，从而未授权访问、使用应用软件、文件和数据的安全风险，需要采用两种或两种以上鉴别方式来，可通过应用系统开发或第三方辅助系统来保证对应用系统登录鉴别安全；

（7）针对应用系统缺陷、接口设计等导致被恶意攻击利用、数据丢失或运行中断而影响服务连续性的安全风险，需要通过对产品采购、自行软件开发、外包软件和测试验收进行流程管理，同时保证应用软件具备自我容错能力；

（8）针对由于应用系统存储数据而引发的数据损毁、丢失等数据安全问题，需通过本地数据备份和异地容灾备份等手段来解决；

（9）针对病毒入侵、恶意代码加载、非授权身份访问等安全威胁，计算设备需要通过采取动态可信验证机制来确保程序运行安全可信，从而保障业务系统安全可信。

4.5安全管理中心安全需求

（1）针对内部管理员的违规操作行为，需要采取身份鉴别、安全审计等技术手段对其操作行为进行限定，并对其相关操作进行审计记录。

（2）针对众多网络设备、安全设备、通信线路等基础设施环境不能有效、统一监测、分析，以及集中安全策略分发、恶意代码特征库、漏洞补丁升级等安全管理问题，需要通过集中安全管控和集中监测审计机制来解决。

（3）针对应用系统过度使用服务器内存、CPU等系统资源的行为，需要对应用软件进行实时的监控管理，同时对系统资源进行管控来解决。

4.6 安全管理制度需求

安全管理制度涉及安全方针、总体安全策略、安全管理制度体系、评审与修订管理等方面。其安全需求如下：

（1）需要制定信息安全工作的总体方针、政策性文件和安全策略等，说明机构安全工作的总体目标、范围、方针、原则、责任等；

1. 需要指定专门的部门对管理活动进行制度化管理，制定相应的制度和操作流程并正式发布；

（3）需要定期对安全管理制度进行评审和修订，不断完善、健全安全制度；

4.7 安全管理机构需求

安全管理机构涉及安全部门设置、人员岗位设置、人员安全管理等方面。其安全需求如下：

（1）需要组建网络安全管理领小组，并设立专门的安全管理工作职能部门，设置相应的管理岗位，配备安全管理人员、审计管理员、系统管理员；

（2）需要建立审批制度，根据岗位职责开展审批和授权相关工作；

（3）需要建立协调机制，就信息安全相关的业务进行协调处理；

（4）需要建立审核和检查部门，安全人员定期的进行全面的安全检查；

（5）需要建立恰当的联络渠道，进行沟通和合作，进行事件的有效处理；

（6）需要建立审核和检查的制度，对安全策略的正确性和安全措施的合理性进行审核和检查；

4.8 安全管理人员需求

（1）需要对人员的录用进行必要的管理，确保人员录用的安全；

（2）需要对人员离岗进行有效的管理，确保人员离岗不会带来安全问题；

（3）需要对人员考核进行严格的管理，提高人员安全技能和安全意识；

（4）需要对人员进行安全意识的教育和培训，提高人员的安全意识；

（5）需要对外部人员进行严格控制，确保外部人员访问受控区域或接入网络时可控可管，并签署保密协议。

4.9 安全建设管理需求

安全建设管理涉及定级备案管理、安全方案设计、产品采购和使用、软件开发管理、安全集成建设、测试验收交付、等级测评以及服务商选择等方面。其安全需求如下：

（1）需要建立备案管理制度，对系统的定级进行备案；

（2）需要具有总体安全方案设计、方案评审的流程和管理能力；

（3）产品采购符合国家有关规定，密码算法和密钥的使用需符合国家密码管理的规定；

（4）需要有专人对工程实施过程进行管理，依据工程实施方案确保安全功能的落地，实（5）施过程需要有第三方工程监理来共同控制实施质量；

（6）需要制定软件开发的相关制度和代码编写规范，并对源代码的安全性进行检测；

（7）需要建立产品采购，系统测试和验收制度，确保安全产品的可信度和产品质量；

（8）需要与符合国家的有关规定的服务供应商签订协议

（9）需要定期组织开展等级测评并及时整改；

（10）需要在工程实施过程中做好文档管理工作，并在系统交付时提供完整的资料交付清单，对运维人员进行技能培训。

4.10 安全运维管理需求

安全运维管理涉及环境管理、资产管理、系统安全运行维护管理、配置与变更管理、安全事件处置及应急响应管理等方面。其安全需求如下：

（1）需要保证机房具有良好的运行环境；

（2）需要建立机房安全管理制度来规范物理访问、物品进出和环境安全；

（3）需要对信息资产进行分类标识、规范化管理；

（4）需要对各种软硬件设备的选型、采购、使用和保管等过程进行控制；

（5）需要各种网络设备、服务器正确使用和维护；

（6）需要采取措施对安全漏洞和隐患进行识别，并及时修补；

（7）需要对网络、操作系统、数据库系统和应用系统进行安全管理；

（8）需要定期地对通信线路进行检查和维护；

（9）需要对恶意代码防范有效性进行验证；

（10）需要对运维工具的使用和远程运维的权限进行管理控制；

（11）需要硬件设备、存储介质存放环境安全，对其使用进行控制和保护；

（12）需要对支撑设施、硬件设备、存储介质进行日常维护和管理；

（13）需要对系统使用手册、维护指南等工具文档进行管理；

（14）需要规范配置管理和变更管理流程；

（15）需要在事件发生后能采取积极、有效的应急策略和措施；

（16）需要建立应急响应机制来应对突发事件，做好应急预案并进行演练；

（17）需要与符合国家有关规定的外包运维服务商签订相关协议，并明确运维服务能力要求。

5 项建设总体目标

为使柘城中医院业务系统安全得到有效保护，按照国家《网络安全法》和《信息安全技术网络安全等级保护》规定的相关要求，在充分解读网络安全等级保护相关政策和标准的基础上，以提升柘城中医院业务系统的安全防护能力，应对新威胁能力为目的，同时利用大数据分析、威胁情报、云防护、物联网安全等新技术理念，建设网络安全管理体系，并达到国家信息安全等级保护的相关标准与要求，最终实现：

（1）重要信息系统（HIS系统）能够顺利通过信息系统（三级）等级保护定级备案。

（2）整个项目建设要求符合中华人民共和国网络安全法相关要求，避免法律责任风险及不良影响。

保障数据安全。预防勒索病毒或业务系统故障，导致的数据丢失或加密问题。

整个项目建设按照体系化的信息安全防护策略进行的整体规划，同时强化风险应对（监测、预警、处置、溯源等）能力，建设一套完整的“事前有防范、事中有应对、事后有追溯”的安全防御体系，合理的安全运营管理，实现新形势下安全管理上台阶、安全技术见实效、综合实力有提升的建设成效，形成具有主动防御和协同运营能力的新一代网络安全保障体系，实现业务系统长期安全稳定的运行，提升信息系统整体的安全保护能力，为高效率、智能和管理等业务工作顺利开展保驾护航。

6项目技术要求

（1）信息系统安全等级保护测评

需要提供1个系统（HIS）定级为等级保护三级的测评服务费用，含专家评审费、相关资料整理与申报、测评、终验。

（2）网络安全等级保护服务

1、按照等保要求，对所有网络设备进行优化(含内、外网闸配置实现物理隔离（网闸利旧、外网核心交换机)，对操作系统和应用系统进行修补、加固和优化。包括针对全网信息平台各种设备、多种操作系统、多项应用的打补丁、停止不必要的服务、升级或更换程序、除去后门程序、修改配置及权限以及针对复杂问题的专门解决方案等服务。

2、按照等保要求，安全管理制度建设。管理制度≥8项、管理机构≥13项、人员管理≥16项、系统建设≥35项，运维管理≥40项，共计≥112项相关制度规范建设。结合现网络情况，整改落实相关流程制度，使之业务上可落地，技术上满足等保要求。

3、在服务期间提供信息安全预警服务（含对应设备/工具）对网络环境进行实时监测并提供应急响应服务；提供每月一次安全检测，形成安全检测报告，采取措施应对发现的安全间题，每季度一次全面安全检查，检查内容包括现有安全技术措施的有效性、安全配置与安全策略的一致性、安全管理制度的执行情况等，包括资产梳理、基线检查、漏洞扫描服务、培训服务、安全分析服务风险评估、应急风险演练。

（3）供配电监测系统

|  |  |  |
| --- | --- | --- |
| **序号** | **功能项** | **技术要求** |
| 1 | 性能要求 | 飞思网巡/DT52，配电系统检测，动力和环境监测供电的模块 |
| 2 | 售后 | 提供三年原厂免费服务 |

1. 机房新风系统

|  |  |  |
| --- | --- | --- |
| **序号** | **功能项** | **技术要求** |
| 1 | 性能要求 | 夏季冬季全年温度23±2℃20±218-28℃  相对湿度45%-65%40%-70%  温度变化率<5℃\h并不得[结露](https://baike.so.com/doc/2044813-2163629.html" \t "https://baike.so.com/doc/_blank)<10℃/h并不得结露主机房内的空气含尘浓度，在表态条件下测试，每升空气中大于或等于0.5μm的尘粒数，应少于18,000粒。 |
| 2 | 部署要求 | 安装完成后须与飞思网巡动环系统联动，达到监测与报警作用。 |
| 3 | 售后服务 | 提供三年原厂免费服务 |

1. 安全加固服务

|  |  |  |
| --- | --- | --- |
| **序号** | **功能项** | **技术要求** |
| 1 | 医院需求 | 对医院整体安全策略进行检查、分析与设计；定期巡检查各项安全设备中策略配置情况，对设备安全策略设置与定期优化、安全设备使用培训、安全制度建立，对违规策略进行必要的优化修改及配置服务。配合厂商进行安全设备使用培训、协助医院完成安全制度建立、消除医院系统安全漏洞、对系统与软件定期升级打补丁工作、定期进行现场安全巡检和组 织应急演练等工作。协助医院通过等保三级。 |
| 2 | 售后服务 | 提供三年原厂免费服务 |

（6）准入控制系统

|  |  |  |
| --- | --- | --- |
| **序号** | **功能项** | **技术要求** |
| 1 | 性能要求 | 双冗余电源，标配≥6个千兆电口，≥8个千兆光口，整机吞吐≥2Gbps，最高支持≥1000个用户准入及管理，提供三年硬件维保服务。 |
| 2 | 授权数量 | 配置≥500个终端设备的准入控制授权，300个基线核查授权。 |
| 3 | 部署要求 | 准入设备应提供客户端的准入模式和无客户端准入模式，可供自定义部署和管理； |
| 4 | 功能要求 | 要求必须支持针对IE弹出窗口等web形式的访问提供入网重定向提示，提示进行客户端注册； 要求提供终端注册的日志记录功能，并可根据时间、设备名、注册者、IP及动作等关键字进行记录查询； ★要求支持注册审核管理功能，已注册终端必须通过管理员审核通过之后才可以接入网络，确保接入内网终端安全可信、可管、可控； ★要求支持本地认证系统，支持自定义本地用户和密码，支持本地认证用户自行修改密码； 支持与AD域服务器、LDAP服务器实现联动认证，并且支持帐户信息的自动同步以及导入导出； 要求支持与Radius认证系统联动进行身份认证，必须支持包含PAP、EAP-MD5、MD5-CHAP等加密认证方式； ★要求支持安检规范定义配置功能，可根据角色属性定制不同的安检规范，安检规范应至少包含杀毒软件安装情况检查、补丁漏洞检查、系统共享资源检查、IE主页修改项检查、guest来宾帐户启用情况检查、远程桌面启用情况检查、系统启动项检查、系统进程检查等； ★要求支持对身份认证通过后的用户终端进行安全检查，并对安检进度提供进度条提示，未通过安检的终端给出未通过项提示并阻断入网，支持安检未通过一键修复功能； 要求支持基于终端心跳和终端水印认证双重准入判断，自动发现采用NAT模式入网的终端并强制认证； 要求支持对路由、无线、AP、HUB等环境下的终端实施准入控制，支持对IPHONE、IPAD等非windows操作系统的终端实施准入控制； ★要求支持外来终端或者访客自助申请上网码，只需要提供管理员要求提供的入网申请资料，便可申请上网码，要求支持管理员自定义入网申请内容； 要求支持访客上网码短信审核功能，管理员无需登录管理平台，只需回复短信就可以对访客入网进行审核,可对访客权限、时间等严格控制； 要求支持对系统本身业务接口的连接状态以及接口速率进行监控，支持对系统本身的CPU以及内存使用率提供仪表盘式图形化实时监控数据，支持数据自动刷新； 支持OEM自定义功能，提供OEM设置接口，管理员可随意更换页面LOGO以满足自身要求； 要求支持系统信息查询，查询内容应包含硬件处理器、内存、硬盘、当前登录管理员、系统时间以及系统当前已运行时长等相关信息，支持查询系统软件序列号、过期时间以及当前系统的软性能参数信息； ★支持网络拓扑发现：通过SNMP、RLOGIN技术，与网络设备联动自动生成网络设备拓扑，协助建立全网网络设备互联可视平台；通过SNMP自身信息，对网络设备性能进行监控，建立网络设备性能监控平台(提供产品截图,加盖厂商公章)； ★支持传统Windows 终端的准入，还支持Linux 终端、摄像头、国产终端、瘦机终端、移动终端，以及网络打印机，网络摄像头等哑终端的指纹识别准入，并能根据策略分类进行终端准入管理(提供产品截图,加盖厂商公章)； ★厂家及产品资质：产品必须同时具备软件著作权证书、公安部销售许可证、中国国家信息安全产品认证证书、全球IPv6论坛IPv6 Ready Logo委员会颁发的IPv6 Ready Logo 认证； |
| 5 | 售后服务 | 提供三年原厂免费服务 |

（7）桌管系统

|  |  |  |
| --- | --- | --- |
| **序号** | **功能项** | **技术要求** |
| 1 | 授权 | 支持不同院区策略级联管理功能，上级管理服务器可强制定制策略并下发给下级管理服务器；下级管理服务器的报警和统计信息级联上报，同时支持上级直接登录下级管理服务器，以进行详细数据查询，要求400+终端,含管理平台。。 |
| 2 | 功能要求 | ★策略漫游功能：当计算机从当前管理器服务器管理区域变换至其它管理器的管理区域后，直接接受该区域管理服务器的接管，并自动获得和执行新管理服务器理的管理策略； 产品拥有自主研发的补丁自动分发功能，不依赖于第三方产品实现，后期支持各国产化操作系统； ★具备补丁内网自动测试功能，即首先分发部分补丁至部分设备，如无问题反馈，待达到设定时间后自动分发至全部设备；对于长期不打补丁的客户端，要求阻止其接入内网的行为；对新接入网络的计算机要求立即安装补丁，否则阻断其入网； 支持对移动存储设备接入管理控制，定义USB标识，必须有专门U盘制作工具对内部U盘进行加密、分区制作管理，根据策略禁止非法USB存储，支持通过移动存储设备认证方式控制本单位与外来移动存储设备的接入； ★必须能够对USB接口中的：音频类、CDC控制类、人机接口类（HID）、物理类、图像类、打印机类、大数据存储类、集线器类、CDC数据类、智能卡类、安全类、诊断设备类、无线控制类、特定应用类及厂商自定义设备等类型的接口进行独立管控（提供截图证明,加盖厂商公章）； 杀毒系统管理：能够识别具有公安部颁发销售许可证的全部杀毒软件，并监控这些防病毒软件在客户端的安装情况、实时运行情况，对未运行杀毒软件的计算机进行如告警、断网处理； 系统支持对受控主机的操作系统、软件和共享等目录中的文件的保护功能，设定访问、删除、修改权限；系统支持对设定目录文件的操作审计，包括文件创建、打印、读写、复制、改名、删除、移动等的记录，同时将信息上报管理信息库供查询； 支持桌面消息通知并回馈，向客户端发送请求重新注册、客户端代理程序升级等消息；能够查询消息回馈情况，了解消息通知接收效果； 支持违规外联管理，防止终端以有线、无线、蓝牙、红外等任何方式连接互联网； ★系统提供安全策略制定功能，根据终端安全防护需要提供安全策略（全局策略、本地策略、备份策略）； ★针对绿色免安装软件，要求能够识别软件的产品名称和源文件名，采用进程指纹、数字签名等特征进行识别和管理，即使进程名称发生改变也能进行管理和控制。对于违规进程采用：不处理、尽提示、断开网络、关机等手段进行管控； ★远程协助。在受管设备用户授权后，通过管理中心远程控制受管设备，完成本地用户所能执行的任何操作，包括屏幕查看、终端事件查看、运行进程查看、终端运行信息资源 查看、当前开放端口查看、安装软件、漏打补丁查看、终端访问审计、终端网络配置修改、关闭终端等。 客户端具有本机软硬件资产统计功能、卸载功能 ； 支持对客户端进行系统安全性审计，包括注册表审计：审计注册表键或者键值是否符合某一条件，对不符合审计要求的键值进行添加或删除；用户密码审计：审计系统用户、网络共享、屏幕保护等密码是否符合规范；用户权限审计：监控系统用户及用户组增加、减少的变化，支持桌面录屏、截屏等审计形式； 厂商资质要求: ★国家信息安全漏洞库技术支撑单位证书三级及以上； ★信息安全等级保护安全建设服务机构能力评估合格证书； ★厂商具有CMMI3级或以上认证证书； ★为体现技术服务实力，须同时具有国家信息安全测评信息安全服务资质安全开发类一级证书和国家信息安全测评信息安全服务资质安全工程类一级证书或以上证书； |
| 3 | 售后服务 | 提供三年原厂免费服务 |

（8）数据库审计系统技术要求

|  |  |  |
| --- | --- | --- |
| **序号** | **功能项** | **技术要求** |
| 1 | 硬件规格 | 双冗余电源，标配≥6个千兆电口。硬盘容量≥2T，授权不少于13个DB服务数，提供三年原厂版本升级及硬件维保服务。 |
| 2 | 性能要求 | 峰值处理能力不低于12000条语句/秒，日志存储能力不低于6亿条， |
| 3 | 功能要求 | ★支持驱动过滤，在流量进入网卡之前对网络流量进行扫描，对无用的信息从网络层进行过滤；避免占用系统资源，系统性能最佳（网络驱动过滤,减少30%资源占用率），提供截图并厂家盖章证明；  ★性能有多级缓存机制，能够在突发流量超出性能设计指标的30%以内流量时，系统能够保证在2个小时内不漏审，提供设计说明并厂家盖章证明； 通过端口镜像（SPAN）或者分流器（TAP）模式旁路部署，无需改造网络、无需在服务器上安装插件、对服务器零干扰、不影响性能、无需服务器账号信息、无需重启服务器、不中断业务； ★支持分布式部署方式，并支持数据库审计集中管理功能，可快速查看所有审计系统的状态、风险状态等，方便区域性管理及防护策略的落实。提供数据库审计分布式管理软件著作权证书并厂家盖章证明； 支持Agent引流，运行时CPU占用率低于3%，内存占用小于100M，程序文件小于2M； ★支持的数据库：Oracle、SQL-Server、DB2、Informix、Sybase、MySQL、PostgreSQL、达梦、人大金仓、南大通用Gbase、神舟、HBase、IP21、Caché、MongoDB、Solr等。提供支持以上数据库功能截图并厂家盖章证明； ★旁路阻断功能（非串联方式）不改变网络结构、不安装插件，设备异常不影响网络，阻断模式具备“严格模式”与“宽松模式”。宽松模式可对单一会话危险操作阻断，危险操作特征外的其他操作不影响；严格模式可对同类型危险操作持续阻断，源IP操作的所有请求直接阻断，提供截图并厂家盖章证明； ★支持Hadoop架构下的大数据库Hbase审计；支持solr全文检索数据库审计；支持HIVE、phoenix等操作工具的审计（要求提供功能效果截图并厂家盖章证明）； ★支持Hive-hwi、Hive-view、Hive-hue，能审计到Hadoop Hive sql创建数据库、建表、删除表、修改表结构、创建／删除视图、向数据表内加载文件、将查询结果插入到Hive表中、基本的查询等操作（要求提供功能效果截图并厂家盖章证明）； ★支持全文检索数据库solr的审计，能审计到solr的查询、插入行为的操作信息（要求提供功能效果截图并厂家盖章证明）； ★支持Hbase的JDBC、Native Java API等接口的调用审计（要求提供功能效果截图并厂家盖章证明）； ★支持基线学习和态势感知，从多维度对数据库安全进行整体分析展现，包括数据库威胁评估、高危操作分析、数据库攻击分析、陌生人闯入分析，提供截图并厂家盖章证明； 系统能自动发现网络中存在的数据库，并自动添加成保护对象进行审计，简化操作，避免用户因模糊记忆引起的配置故障； ★对图形界面运维工具检索后再删除检索出的记录，能够审计到删除的具体记录内容，提供截图并厂家盖章证明； 支持B/S应用系统三层架构http应用审计，可提取包括应用系统的人员工号（账号）在内的“六元组”身份信息，精确定位到人，并可获取XML返回结果；支持框架：tomcat、apache、weblogic、jboss； 支持带COM、COM+、DCOM组件的三层架构应用审计，可提取包括应用层工号（账号）之内的“六元组”身份信息，精确定位到人； 审计策略支持18种以上分项响应条件；可支持数据库操作命令（包括select、create等14个命令）；语句长度、语句执行回应、语句执行时间、返回内容、返回行数、数据库名、数据库账户、服务器端口、客户端操作系统主机名、客户端操作系统用户名、客户端MAC、客户端IP、客户端端口、客户端进程名、会话ID、关键字、时间（含开始结束日期）等； ★内置疑似SQL注入、跨站脚本攻击、数据库导库、字段猜测、代码更改、等近百种高危风险审计规则库，无需单独配置，直接调用（要求提供功能截图并厂家盖章证明）； ★支持操作语句系列的组合审计规则，可根据某一客体的操作行为序列，连续操作了设定的语句序列时进行规则审计告警，提供截图并厂家盖章证明； ★支持重复操作的统计审计规则，可根据在一定的时间内，重复某项操作达到设定的统计次数进行规则审计告警，提供截图并厂家盖章证明； 支持对HTTP、telent、snmp/pop3、NFS协议审计； 支持全数据库检索，检索效率高达亿条数据秒级响应，快速定位相应的审计会话内容； 可根据事件的时间范围、客户端IP、关键字、进程名、数据库账号、规则名、客户端端口号、返回内容等多种条件进行事件回放，回溯事件过程； 支持自定义报表，客户可根据需求定义报表的统计内容，报表支持塞班斯（SOX）法案、等级保护标准要求生成多维度综合报告；支持按照源IP地址、客户端工具、帐号、告警数等源信息生成报表；支持按照数据库访问行为生成报表；可自定义条件生成报表； ★对审计记录返回内容中的敏感数据能进行隐秘处理，防止二次泄露（要求提供功能截图并厂家盖章证明）； 管理员登陆支持静态口令认证，密码短信认证。支持密码的复杂性管理，支持限制登录时间、登录次数、锁定用户时间、超时退出时间、密码最短长度、密码最长长度、密码过期时间、密码过期状态； 系统本身具备访问防火墙，对于系统的异常访问可对账号进行强制下线管理，能有效防范非法IP地址、防范暴力破解登录用户密码（能够对连续失败登陆进行自动锁定，锁定时间可设置）、设置系统黑白名单等安全功能； 提供用户界面告警、Syslog告警、SNMP告警、邮件告警、短信告警五种方式； 可提供审计策略和配置数据的导入导出功能，可提供风险审计记录的导入导出，支持根据保留天数和占用百分比自动清理，提供审计数据管理功能，能够实现对审计数据的自动备份、手动备份，支持增量、全量备份方式，备份数据可自动存储在指定的FTP服务器上； 日志信息支持通过API接口或syslog、SNMP等协议发送到第三方日志管理平台统一管理； ★所投产品具有《计算机信息系统安全专用产品销售许可证（增强型）》、《涉密信息系统产品检测证书》、《中国国家信息安全产品认证证书（增强型）》需提供相关证书复印件并厂家盖章； ★所投产品具有《应用审计系统》、《面向多类型数据库的高性能审计系统》、《数据库安全审计系统》、《网络安全审计软件》计算机软件著作权登记证书，需提供相关证书复印件并厂家盖章； 提供所投产品厂商过往同类项目业绩，并在投标文件中附有其合同加盖供应商红色公章的复印件（包含附件）；同类项目业绩是指合同中含有数据库审计系统审计功能支持Hadoop架构下的大数据库Hbase审计或支持Hive-hwi、Hive-view、Hive-hue或支持全文检索数据库solr的审计或支持Hbase的JDBC、Native Java API等接口的调用审计或支持CACHE非关系型数据库审计的业绩；合同原件备查； |
| 3 | 售后服务 | 提供三年原厂免费服务 |

（9）数据备份软件

|  |  |  |
| --- | --- | --- |
| **序号** | **功能项** | **技术要求** |
| 1 | 主要功能 | 配置HIS、emr、pacs、lis核心业务系统备份许可（每个许可都包含文件和数据库的备份恢复、连续数据复制保护、lanfree备份功能）； |
| 2 | 功能要求 | 支持文件、Oracle数据库、邮件系统备份/恢复断点续备功能，自动从断点处重起续传，免人工干预；  具有文件系统及相关应用连续数据复制保护，并能创建应用一致点快照，数据丢失少并确保应用一致性，满足用户备份的ROP/RTO要求；  只传送在目标端没有的数据块，传输的数据量小，节省时间和网络带宽。能够在指定的时间点/时间段调度异地拷贝计划，时间控制灵活。能够选择部分数据复制，不是将所有的已备份数据全部复制。源拷贝和异地拷贝可以设置不同的保留时间。异地拷贝是原拷贝的副本，当原拷贝不能使用时可以用异地拷贝来恢复数据；  按定义的策略对不经常使用的虚拟机自动关机，对一段时间不开机的虚机自动归档到二级存储，需要访问时可恢复归档虚拟机，以降低主存储成本及释放虚拟服务器资源；  ★软件提供防勒索病毒功能 ，阻止任何非法进程修改备份数据，避免备份数据被破坏导致的无法恢复，提供功能截图证明；  不需要恢复虚拟机备份数据，可直接运行备份虚拟机，并可选择同时进行后台恢复。 |
| 3 | 售后服务 | 提供三年原厂免费服务。 |

# 第五章 投标文件格式

柘城中医院有限公司

信息系统安全等级保护（三级）建设项目

投 标 文 件

投标人： （盖单位章）

法定代表人或其委托代理人： （签字）

年 月 日

**目 录**

一、投标函及投标函附录

二、法定代表人身份证明及授权委托书

三、已标价建设内容清单

四、技术参数偏离表

五、项目设计与实施方案

六、项目管理机构

七、资格审查资料

八、招标品牌要求及投标品牌反馈表

八、项目班子到岗履职承诺书

九、柘城中医院新冠肺炎疫情防控承诺书

## 一、投标函及投标函附录

### （一）投标函

（招标人名称）：

1．我方已仔细研究了 （项目名称）招标文件的全部内容，愿意以人民币（大写） （¥ ）的投标总报价，实施工期 日历天，按合同约定实施和完成本项目内容，取得信息安全等级保护（三级）备案证书。

2．我方承诺在招标文件规定的投标有效期内不修改、撤销投标文件。

3．随同本投标函提交投标保证金一份，金额为人民币（大写） / （¥ / ）。

4．如我方中标：

（1）我方承诺在收到中标通知书后，在中标通知书规定的期限内与你方签订合同。

（2）随同本投标函递交的投标函附录属于合同文件的组成部分。

（3）我方承诺按照招标文件规定向你方递交履约担保。

（4）我方承诺在合同约定的期限内完成并全部合同约定建设项目。

5．我方在此声明，所递交的投标文件及有关资料内容完整、真实和准确，且不存在第二章“投标人须知”第1.4.3项和第1.4.4项规定的任何一种情形。

6. （其他补充说明）。

投 标 人： （盖单位章）

法定代表人或其委托代理人： （签字）

地址：

电话：

传真：

邮政编码：

年 月 日

### （二）投标函附录

|  |  |  |  |
| --- | --- | --- | --- |
| **序号** | **条款名称** | **约定内容** | **是否响应** |
| 1 | 项目经理 |  |  |
| 2 | 实施工期 |  |  |
| 3 | 投标有效期 | 90天 |  |
| 4 | 转包 | 不转包 |  |
| 5 | 权利义务 | 符合第三章“合同条款及格式”规定 |  |
| 6 | 技术标准和要求 | 符合第四章“技术标准和要求”规定。 |  |
| 7 | 质量保证金 | 见投标人须知规定。 |  |
| 备注：投标人在响应招标文件中规定的实质性要求和条件的基础上，可做出其他有利于招标人的承诺。此类承诺可在本表中予以补充填写。 | | | |

**投标人**（盖章）：

**法人代表或委托代理人**（签字或盖章）：

**日期： 年 月 日**

## 二、法定代表人身份证明及授权委托书

### （一）法定代表人身份证明

投标人名称：

单位性质：

地址：

成立时间： 年 月 日

经营期限：

姓名： 性别： 年龄： 职务：

系 （投标人名称）的法定代表人。

特此证明。

投标人： （盖单位章）

年 月 日

### （二）授权委托书

本人 （姓名）系 （投标人名称）的法定代表人，现委托 （姓名）为我方代理人。代理人根据授权，以我方名义签署、澄清、说明、补正、递交、撤回、修改 \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ （项目名称）投标文件、签订合同和处理有关事宜，其法律后果由我方承担。

委托期限： 。

代理人无转委托权。

附：法定代表人身份证和被授权人身份证复印件加盖公章

投标人： （盖单位章）

法定代表人： （签字）

身份证号码：

委托代理人： （签字）

身份证号码：

年 月 日

## 三、已标价建设内容清单

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 序号 | 项目/设备 名称 | 详细参数（型号、配置） | 品牌 | 保修及服务期限 | 数量 | 单价 | 报价 |
| 1 | 信息系统安全等级保护测评 | HIS系统（三级）专家评审费、相关资料整理与申报、测评、终验。 |  | 1年 | 1 |  |  |
| 2 | 供配电监测系统 |  |  | 3年 | 2 |  |  |
| 3 | 准入控制系统 |  |  | 3年 | 1 |  |  |
| 4 | 机房新风系统 |  |  | 3年 | 1 |  |  |
| 5 | 数据库审计系统 |  |  | 3年 | 1 |  |  |
| 6 | 桌管系统 |  |  | 3年 | 1 |  |  |
| 7 | 数据备份软件 |  |  | 3年 | 1 |  |  |
| 8 | 安全加固服务 |  |  | 1年 | 1 |  |  |
|  | 项目总计（单位：元） | | | | | |  | |

## 四、技术参数偏离表

（1）等级保护（三级）测评

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **序号** | **功能项** | **技术要求** | **是否偏离** | **偏离说明** |
| 1 | 测评系统要求 | （HIS、互联网医院）定级为等级保护三级的测评服务 |  | 不允许偏离 |
| 2 | 性能及技术要求 | 含专家评审费、相关资料整理与申报、测评、终验。 |  | 不允许偏离 |
| 3 | 完成期限≦ 90天 |  | 可以正向偏离 |

（2）网络安全等级保护服务

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **序号** | **功能项** | **技术要求** | **是否偏离** | **偏离说明** |
| 1 | 安全服务 | ▲按照等保要求，对所有网络设备进行优化(含内、外网闸配置实现物理隔离（网闸利旧暂未上架）、外网核心交换机（未上架设备利旧）更换优化)，对操作系统和应用系统进行修补、加固和优化。包括针对全网信息平台各种设备、多种操作系统、多项应用的打补丁、停止不必要的服务、升级或更换程序、除去后门程序、修改配置及权限以及针对复杂问题的专门解决方案等服务。 |  | 不允许偏离 |
| 2 | ▲在服务期间提供信息安全预警服务（含对应设备/工具）对网络环境进行实时监测并提供应急响应服务；提供每月一次安全检测，形成安全检测报告，采取措施应对发现的安全间题，每季度一次全面安全检查，检查内容包括现有安全技术措施的有效性、安全配置与安全策略的一致性、安全管理制度的执行情况等，包括资产梳理、基线检查、漏洞扫描服务、培训服务、安全分析服务风险评估、应急风险演练。 |  | 不允许偏离 |
| 3 | 制度建设 | ▲按照等保要求，安全管理制度建设。管理制度≥8项、管理机构≥13项、人员管理≥16项、系统建设≥35项，运维管理≥40项，共计≥112项相关制度规范建设。结合现网络情况，整改落实相关流程制度，使之业务上可落地，技术上满足等保要求。 |  | 不允许偏离 |

（3）供配电监测系统

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **序号** | **功能项** | **技术要求** | **是否偏离** | **偏离说明** |
| 1 | 性能要求 | 飞思网巡/DT52，配电系统检测，动力和环境监测供电的模块 |  |  |
| 2 | 售后服务 | 提供三年原厂免费服务 |  |  |

（4）机房新风系统

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **序号** | **功能项** | **技术要求** | **是否偏离** | **偏离说明** |
| 1 | 性能要求 | 夏季冬季全年温度23±2℃20±218-28℃  相对湿度45%-65%40%-70%  温度变化率<5℃\h并不得[结露](https://baike.so.com/doc/2044813-2163629.html" \t "https://baike.so.com/doc/_blank)<10℃/h并不得结露主机房内的空气含尘浓度，在表态条件下测试，每升空气中大于或等于0.5μm的尘粒数，应少于18,000粒。 |  |  |
| 2 | 部署要求 | 安装完成后须与飞思网巡动环系统联动，达到监测与报警作用。 |  |  |
| 3 | 售后服务 | 提供三年原厂免费服务 |  |  |

（5）安全加固服务

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **序号** | **功能项** | **技术要求** | **是否偏离** | **偏离说明** |
| 1 | 医院需求 | 对医院整体安全策略进行检查、分析与设计；定期巡检查各项安全设备中策略配置情况，对设备安全策略设置与定期优化、安全设备使用培训、安全制度建立，对违规策略进行必要的优化修改及配置服务。配合厂商进行安全设备使用培训、协助医院完成安全制度建立、消除医院系统安全漏洞、对系统与软件定期升级打补丁工作、定期进行现场安全巡检和组 织应急演练等工作。协助医院通过等保三级。 |  |  |
| 2 | 售后服务 | 提供三年原厂免费服务 |  |  |

（6）准入控制系统

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **序号** | **功能项** | **技术要求** | **是否偏离** | **偏离说明** |
| 1 | 性能要求 | 双冗余电源，标配≥6个千兆电口，≥8个千兆光口，整机吞吐≥2Gbps，最高支持≥1000个用户准入及管理，提供三年硬件维保服务。 |  |  |
| 2 | 授权数量 | 配置≥500个终端设备的准入控制授权，300个基线核查授权。 |  |  |
| 3 | 部署要求 | 准入设备应提供客户端的准入模式和无客户端准入模式，可供自定义部署和管理； |  |  |
| 4 | 功能要求 | 要求必须支持针对IE弹出窗口等web形式的访问提供入网重定向提示，提示进行客户端注册； 要求提供终端注册的日志记录功能，并可根据时间、设备名、注册者、IP及动作等关键字进行记录查询； ★要求支持注册审核管理功能，已注册终端必须通过管理员审核通过之后才可以接入网络，确保接入内网终端安全可信、可管、可控； ★要求支持本地认证系统，支持自定义本地用户和密码，支持本地认证用户自行修改密码； 支持与AD域服务器、LDAP服务器实现联动认证，并且支持帐户信息的自动同步以及导入导出； 要求支持与Radius认证系统联动进行身份认证，必须支持包含PAP、EAP-MD5、MD5-CHAP等加密认证方式； ★要求支持安检规范定义配置功能，可根据角色属性定制不同的安检规范，安检规范应至少包含杀毒软件安装情况检查、补丁漏洞检查、系统共享资源检查、IE主页修改项检查、guest来宾帐户启用情况检查、远程桌面启用情况检查、系统启动项检查、系统进程检查等； ★要求支持对身份认证通过后的用户终端进行安全检查，并对安检进度提供进度条提示，未通过安检的终端给出未通过项提示并阻断入网，支持安检未通过一键修复功能； 要求支持基于终端心跳和终端水印认证双重准入判断，自动发现采用NAT模式入网的终端并强制认证； 要求支持对路由、无线、AP、HUB等环境下的终端实施准入控制，支持对IPHONE、IPAD等非windows操作系统的终端实施准入控制； ★要求支持外来终端或者访客自助申请上网码，只需要提供管理员要求提供的入网申请资料，便可申请上网码，要求支持管理员自定义入网申请内容； 要求支持访客上网码短信审核功能，管理员无需登录管理平台，只需回复短信就可以对访客入网进行审核,可对访客权限、时间等严格控制； 要求支持对系统本身业务接口的连接状态以及接口速率进行监控，支持对系统本身的CPU以及内存使用率提供仪表盘式图形化实时监控数据，支持数据自动刷新； 支持OEM自定义功能，提供OEM设置接口，管理员可随意更换页面LOGO以满足自身要求； 要求支持系统信息查询，查询内容应包含硬件处理器、内存、硬盘、当前登录管理员、系统时间以及系统当前已运行时长等相关信息，支持查询系统软件序列号、过期时间以及当前系统的软性能参数信息； ★支持网络拓扑发现：通过SNMP、RLOGIN技术，与网络设备联动自动生成网络设备拓扑，协助建立全网网络设备互联可视平台；通过SNMP自身信息，对网络设备性能进行监控，建立网络设备性能监控平台(提供产品截图,加盖厂商公章)； ★支持传统Windows 终端的准入，还支持Linux 终端、摄像头、国产终端、瘦机终端、移动终端，以及网络打印机，网络摄像头等哑终端的指纹识别准入，并能根据策略分类进行终端准入管理(提供产品截图,加盖厂商公章)； ★厂家及产品资质：产品必须同时具备软件著作权证书、公安部销售许可证、中国国家信息安全产品认证证书、全球IPv6论坛IPv6 Ready Logo委员会颁发的IPv6 Ready Logo 认证； |  |  |
| 5 | 售后服务 | 提供三年原厂免费服务 |  |  |

（7）桌管系统

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **序号** | **功能项** | **技术要求** | **是否偏离** | **偏离说明** |
| 1 | 授权 | 支持不同院区策略级联管理功能，上级管理服务器可强制定制策略并下发给下级管理服务器；下级管理服务器的报警和统计信息级联上报，同时支持上级直接登录下级管理服务器，以进行详细数据查询，要求400+终端,含管理平台。。 |  |  |
| 2 | 功能要求 | ★策略漫游功能：当计算机从当前管理器服务器管理区域变换至其它管理器的管理区域后，直接接受该区域管理服务器的接管，并自动获得和执行新管理服务器理的管理策略； 产品拥有自主研发的补丁自动分发功能，不依赖于第三方产品实现，后期支持各国产化操作系统； ★具备补丁内网自动测试功能，即首先分发部分补丁至部分设备，如无问题反馈，待达到设定时间后自动分发至全部设备；对于长期不打补丁的客户端，要求阻止其接入内网的行为；对新接入网络的计算机要求立即安装补丁，否则阻断其入网； 支持对移动存储设备接入管理控制，定义USB标识，必须有专门U盘制作工具对内部U盘进行加密、分区制作管理，根据策略禁止非法USB存储，支持通过移动存储设备认证方式控制本单位与外来移动存储设备的接入； ★必须能够对USB接口中的：音频类、CDC控制类、人机接口类（HID）、物理类、图像类、打印机类、大数据存储类、集线器类、CDC数据类、智能卡类、安全类、诊断设备类、无线控制类、特定应用类及厂商自定义设备等类型的接口进行独立管控（提供截图证明,加盖厂商公章）； 杀毒系统管理：能够识别具有公安部颁发销售许可证的全部杀毒软件，并监控这些防病毒软件在客户端的安装情况、实时运行情况，对未运行杀毒软件的计算机进行如告警、断网处理； 系统支持对受控主机的操作系统、软件和共享等目录中的文件的保护功能，设定访问、删除、修改权限；系统支持对设定目录文件的操作审计，包括文件创建、打印、读写、复制、改名、删除、移动等的记录，同时将信息上报管理信息库供查询； 支持桌面消息通知并回馈，向客户端发送请求重新注册、客户端代理程序升级等消息；能够查询消息回馈情况，了解消息通知接收效果； 支持违规外联管理，防止终端以有线、无线、蓝牙、红外等任何方式连接互联网； ★系统提供安全策略制定功能，根据终端安全防护需要提供安全策略（全局策略、本地策略、备份策略）； ★针对绿色免安装软件，要求能够识别软件的产品名称和源文件名，采用进程指纹、数字签名等特征进行识别和管理，即使进程名称发生改变也能进行管理和控制。对于违规进程采用：不处理、尽提示、断开网络、关机等手段进行管控； ★远程协助。在受管设备用户授权后，通过管理中心远程控制受管设备，完成本地用户所能执行的任何操作，包括屏幕查看、终端事件查看、运行进程查看、终端运行信息资源 查看、当前开放端口查看、安装软件、漏打补丁查看、终端访问审计、终端网络配置修改、关闭终端等。 客户端具有本机软硬件资产统计功能、卸载功能 ； 支持对客户端进行系统安全性审计，包括注册表审计：审计注册表键或者键值是否符合某一条件，对不符合审计要求的键值进行添加或删除；用户密码审计：审计系统用户、网络共享、屏幕保护等密码是否符合规范；用户权限审计：监控系统用户及用户组增加、减少的变化，支持桌面录屏、截屏等审计形式； 厂商资质要求: ★国家信息安全漏洞库技术支撑单位证书三级及以上； ★信息安全等级保护安全建设服务机构能力评估合格证书； ★厂商具有CMMI3级或以上认证证书； ★为体现技术服务实力，须同时具有国家信息安全测评信息安全服务资质安全开发类一级证书和国家信息安全测评信息安全服务资质安全工程类一级证书或以上证书； |  |  |
| 3 | 售后服务 | 提供三年原厂免费服务 |  |  |

（8）数据库审计系统技术要求

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **序号** | **功能项** | **技术要求** | **是否偏离** | **偏离说明** |
| 1 | 硬件规格 | 双冗余电源，标配≥6个千兆电口。硬盘容量≥2T，授权不少于13个DB服务数，提供三年原厂版本升级及硬件维保服务。 |  |  |
| 2 | 性能要求 | 峰值处理能力不低于12000条语句/秒，日志存储能力不低于6亿条， |  |  |
| 3 | 功能要求 | ★支持驱动过滤，在流量进入网卡之前对网络流量进行扫描，对无用的信息从网络层进行过滤；避免占用系统资源，系统性能最佳（网络驱动过滤,减少30%资源占用率），提供截图并厂家盖章证明；  ★性能有多级缓存机制，能够在突发流量超出性能设计指标的30%以内流量时，系统能够保证在2个小时内不漏审，提供设计说明并厂家盖章证明； 通过端口镜像（SPAN）或者分流器（TAP）模式旁路部署，无需改造网络、无需在服务器上安装插件、对服务器零干扰、不影响性能、无需服务器账号信息、无需重启服务器、不中断业务； ★支持分布式部署方式，并支持数据库审计集中管理功能，可快速查看所有审计系统的状态、风险状态等，方便区域性管理及防护策略的落实。提供数据库审计分布式管理软件著作权证书并厂家盖章证明； 支持Agent引流，运行时CPU占用率低于3%，内存占用小于100M，程序文件小于2M； ★支持的数据库：Oracle、SQL-Server、DB2、Informix、Sybase、MySQL、PostgreSQL、达梦、人大金仓、南大通用Gbase、神舟、HBase、IP21、Caché、MongoDB、Solr等。提供支持以上数据库功能截图并厂家盖章证明； ★旁路阻断功能（非串联方式）不改变网络结构、不安装插件，设备异常不影响网络，阻断模式具备“严格模式”与“宽松模式”。宽松模式可对单一会话危险操作阻断，危险操作特征外的其他操作不影响；严格模式可对同类型危险操作持续阻断，源IP操作的所有请求直接阻断，提供截图并厂家盖章证明； ★支持Hadoop架构下的大数据库Hbase审计；支持solr全文检索数据库审计；支持HIVE、phoenix等操作工具的审计（要求提供功能效果截图并厂家盖章证明）； ★支持Hive-hwi、Hive-view、Hive-hue，能审计到Hadoop Hive sql创建数据库、建表、删除表、修改表结构、创建／删除视图、向数据表内加载文件、将查询结果插入到Hive表中、基本的查询等操作（要求提供功能效果截图并厂家盖章证明）； ★支持全文检索数据库solr的审计，能审计到solr的查询、插入行为的操作信息（要求提供功能效果截图并厂家盖章证明）； ★支持Hbase的JDBC、Native Java API等接口的调用审计（要求提供功能效果截图并厂家盖章证明）； ★支持基线学习和态势感知，从多维度对数据库安全进行整体分析展现，包括数据库威胁评估、高危操作分析、数据库攻击分析、陌生人闯入分析，提供截图并厂家盖章证明； 系统能自动发现网络中存在的数据库，并自动添加成保护对象进行审计，简化操作，避免用户因模糊记忆引起的配置故障； ★对图形界面运维工具检索后再删除检索出的记录，能够审计到删除的具体记录内容，提供截图并厂家盖章证明； 支持B/S应用系统三层架构http应用审计，可提取包括应用系统的人员工号（账号）在内的“六元组”身份信息，精确定位到人，并可获取XML返回结果；支持框架：tomcat、apache、weblogic、jboss； 支持带COM、COM+、DCOM组件的三层架构应用审计，可提取包括应用层工号（账号）之内的“六元组”身份信息，精确定位到人； 审计策略支持18种以上分项响应条件；可支持数据库操作命令（包括select、create等14个命令）；语句长度、语句执行回应、语句执行时间、返回内容、返回行数、数据库名、数据库账户、服务器端口、客户端操作系统主机名、客户端操作系统用户名、客户端MAC、客户端IP、客户端端口、客户端进程名、会话ID、关键字、时间（含开始结束日期）等； ★内置疑似SQL注入、跨站脚本攻击、数据库导库、字段猜测、代码更改、等近百种高危风险审计规则库，无需单独配置，直接调用（要求提供功能截图并厂家盖章证明）； ★支持操作语句系列的组合审计规则，可根据某一客体的操作行为序列，连续操作了设定的语句序列时进行规则审计告警，提供截图并厂家盖章证明； ★支持重复操作的统计审计规则，可根据在一定的时间内，重复某项操作达到设定的统计次数进行规则审计告警，提供截图并厂家盖章证明； 支持对HTTP、telent、snmp/pop3、NFS协议审计； 支持全数据库检索，检索效率高达亿条数据秒级响应，快速定位相应的审计会话内容； 可根据事件的时间范围、客户端IP、关键字、进程名、数据库账号、规则名、客户端端口号、返回内容等多种条件进行事件回放，回溯事件过程； 支持自定义报表，客户可根据需求定义报表的统计内容，报表支持塞班斯（SOX）法案、等级保护标准要求生成多维度综合报告；支持按照源IP地址、客户端工具、帐号、告警数等源信息生成报表；支持按照数据库访问行为生成报表；可自定义条件生成报表； ★对审计记录返回内容中的敏感数据能进行隐秘处理，防止二次泄露（要求提供功能截图并厂家盖章证明）； 管理员登陆支持静态口令认证，密码短信认证。支持密码的复杂性管理，支持限制登录时间、登录次数、锁定用户时间、超时退出时间、密码最短长度、密码最长长度、密码过期时间、密码过期状态； 系统本身具备访问防火墙，对于系统的异常访问可对账号进行强制下线管理，能有效防范非法IP地址、防范暴力破解登录用户密码（能够对连续失败登陆进行自动锁定，锁定时间可设置）、设置系统黑白名单等安全功能； 提供用户界面告警、Syslog告警、SNMP告警、邮件告警、短信告警五种方式； 可提供审计策略和配置数据的导入导出功能，可提供风险审计记录的导入导出，支持根据保留天数和占用百分比自动清理，提供审计数据管理功能，能够实现对审计数据的自动备份、手动备份，支持增量、全量备份方式，备份数据可自动存储在指定的FTP服务器上； 日志信息支持通过API接口或syslog、SNMP等协议发送到第三方日志管理平台统一管理； ★所投产品具有《计算机信息系统安全专用产品销售许可证（增强型）》、《涉密信息系统产品检测证书》、《中国国家信息安全产品认证证书（增强型）》需提供相关证书复印件并厂家盖章； ★所投产品具有《应用审计系统》、《面向多类型数据库的高性能审计系统》、《数据库安全审计系统》、《网络安全审计软件》计算机软件著作权登记证书，需提供相关证书复印件并厂家盖章； 提供所投产品厂商过往同类项目业绩，并在投标文件中附有其合同加盖供应商红色公章的复印件（包含附件）；同类项目业绩是指合同中含有数据库审计系统审计功能支持Hadoop架构下的大数据库Hbase审计或支持Hive-hwi、Hive-view、Hive-hue或支持全文检索数据库solr的审计或支持Hbase的JDBC、Native Java API等接口的调用审计或支持CACHE非关系型数据库审计的业绩；合同原件备查； |  |  |
| 3 | 售后服务 | 提供三年原厂免费服务 |  |  |

（9）数据备份软件

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **序号** | **功能项** | **技术要求** | **是否偏离** | **偏离说明** |
| 1 | 主要功能 | 配置HIS、emr、pacs、lis核心业务系统备份许可（每个许可都包含文件和数据库的备份恢复、连续数据复制保护、lanfree备份功能）； |  |  |
| 2 | 功能要求 | 支持文件、Oracle数据库、邮件系统备份/恢复断点续备功能，自动从断点处重起续传，免人工干预；  具有文件系统及相关应用连续数据复制保护，并能创建应用一致点快照，数据丢失少并确保应用一致性，满足用户备份的ROP/RTO要求；  只传送在目标端没有的数据块，传输的数据量小，节省时间和网络带宽。能够在指定的时间点/时间段调度异地拷贝计划，时间控制灵活。能够选择部分数据复制，不是将所有的已备份数据全部复制。源拷贝和异地拷贝可以设置不同的保留时间。异地拷贝是原拷贝的副本，当原拷贝不能使用时可以用异地拷贝来恢复数据；  按定义的策略对不经常使用的虚拟机自动关机，对一段时间不开机的虚机自动归档到二级存储，需要访问时可恢复归档虚拟机，以降低主存储成本及释放虚拟服务器资源；  ★软件提供防勒索病毒功能 ，阻止任何非法进程修改备份数据，避免备份数据被破坏导致的无法恢复，提供功能截图证明；  不需要恢复虚拟机备份数据，可直接运行备份虚拟机，并可选择同时进行后台恢复。 |  |  |
| 3 | 售后服务 | 提供三年原厂免费服务。 |  |  |

## 五、项目设计与实施方案

1．投标人应根据招标文件和对现场的调研情况，依据招标文件评标办法2.2设计评分标准对应的具体得分项目采用文字并结合图表的形式进行编制。

目录如下：

1、项目概述（背景、技术标准、建设目标）

2、网络安全现况与需求分析（风险分析、需求分析）

4、方案总体设计（设计原则、核心网络拓扑图（注：互联网接入防火墙与内网核心交换机中间设计增加一台网闸（设备院方提供，不列入本次项目设备清单））的布署方案、安全技术设计(内外网准入设计、内外网入侵检测设计)、提供安全运维服务标准）

5、项目实施周期计划（从项目启至取得HIS系统、互联网医院信息安全等级保护（三级）备案证书止，期间各环节实施工作计划）。

## 六、项目管理机构

### （一）项目管理机构组成表

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 职务 | 姓名 | 职称 | 执业或职业资格证明 | | | | 备注 |
| 证书名称 | 级别 | 证号 | 养老保险 |  |
| 项目经理 |  |  |  |  |  |  |  |
|  |  |  |
|  |  |  |
| 实施人员 |  |  |  |  |  |  |  |
|  |  |  |
| 实施人员 |  |  |  |  |  |  |  |
|  |  |  |

（二）项目经理简历表

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 姓 名 |  | 年 龄 |  | | 学历 |  |
| 职 称 |  | 职 务 |  | | 拟在本合同任职 |  |
| 毕业学校 | 年毕业于 学校 专业 | | | | | |
| 主要工作经历 | | | | | | |
| 时 间 | 参加过的类似项目 | | | 查询网址 | 担任职务 | 发包人及联系电话 |
|  |  | | |  |  |  |
|  |  | | |  |  |  |
|  |  | | |  |  |  |
|  |  | | |  |  |  |
|  |  | | |  |  |  |
|  |  | | |  |  |  |
|  |  | | |  |  |  |
|  |  | | |  |  |  |

应附中级及以上网络工程师认证、IT服务项目经理认证或IT服务工程师认证、信息安全等保2.0认证证书等复印件加盖公章，社保缴费证明（6个月）复印件。

承诺书

————————（招标人名称）：

我方在此声明，我方拟派往 （项目名称） （以下简称“本工程”）的项目经理 （项目经理姓名）现阶段没有担任任何在施建设工程项目的项目经理。

我方保证上述信息的真实和准确，并愿意承担因我方就此弄虚作假所引起的一切法律后果。

特此承诺

投标人： （盖单位章）

法定代表人： （签字或盖章）

项目经理： （签字）

年 月 日

### （三）主要项目管理人员简历表

项目经理应具备项目管理、网络安全、IT 服务的能力，在同时具有中级及以上网络工程师认证、IT服务项目经理认证或IT服务工程师认证、信息安全等保2.0认证。有实施过相关项目案例。应附注册资格证书（或职称证）复印件加盖公章，社保缴费证明复印件。

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 岗位名称 | |  | | | |
| 姓 名 | |  | 年 龄 |  | |
| 性 别 | |  | 专业职称 |  | |
| 拥有的资格 | |  | 工作年限 |  | |
| 主  要  工  作  业  绩  及  担  任  的  主  要  工  作 |  | | | |

## 七、资格审查资料

### （一）投标人基本情况表

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 投标人名称 |  | | | | | | | | |
| 注册地址 |  | | | | 邮政编码 | |  | | |
| 联系方式 | 联系人 |  | | | 电 话 | |  | | |
| 传 真 |  | | | 网 址 | |  | | |
| 组织结构 |  | | | | | | | | |
| 法定代表人 | 姓名 |  | 技术职称 |  | | 电话 | |  | |
| 技术负责人 | 姓名 |  | 技术职称 |  | | 电话 | |  | |
| 成立时间 |  | | 员工总人数： | | | | | | |
| 企业资质等级 |  | | 其中 | 项目经理 | | | | |  |
| 营业执照号 |  | | 高级职称人员 | | | | |  |
| 注册资金 |  | | 中级职称人员 | | | | |  |
| 开户银行 |  | | 初级职称人员 | | | | |  |
| 账号 |  | | 技 工 | | | | |  |
| 经营范围 |  | | | | | | | | |
| 备注 |  | | | | | | | | |

备注：本表后应附企业法人营业执照副本、企业资质证书副本、税务登记证副本、组织机构代码证副本、开户行许可证等材料的复印件加盖公章。

### （二）近年财务状况表

备注：在此附经会计师事务所审计的财务会计报表，包括资产负债表、损益表、现金流量表、利润表和财务情况说明书的复印件加盖公章，具体年份要求见第一章“投标人须知”的规定。

### （三）近年完成的类似项目情况表

|  |  |
| --- | --- |
| 项目名称 |  |
| 项目所在地 |  |
| 发包人名称 |  |
| 发包人地址 |  |
| 发包人电话 |  |
| 合同价格 |  |
| 开工日期 |  |
| 竣工日期 |  |
| 承担的工作 |  |
| 项目经理 |  |
| 技术负责人 |  |
| 项目描述 |  |
| 查询网址 |  |
| 备注 |  |

### （四）正在实施的和新承接的项目情况表

|  |  |
| --- | --- |
| 项目名称 |  |
| 项目所在地 |  |
| 发包人名称 |  |
| 发包人地址 |  |
| 发包人电话 |  |
| 签约合同价 |  |
| 开工日期 |  |
| 计划竣工日期 |  |
| 承担的工作 |  |
| 项目经理 |  |
| 技术负责人 |  |
| 项目描述 |  |
| 备注 |  |

备注：本表后附中标通知书和合同协议书复印件加盖公章。每张表格只填写一个项目，并标明序号。

### （五）近年发生的诉讼和仲裁情况

说明：近年发生的诉讼和仲裁情况仅限于投标人败诉的，且与履行施工承包合同有关的案件，不包括调解结案以及未裁决的仲裁或未终审判决的诉讼。

### （六）企业其他信誉情况表（年份要求同诉讼及仲裁情况年份要求）

1、近年企业不良行为记录情况

2、在施工程以及近年已竣工工程合同履行情况

3、其 他

备注：1、企业不良行为记录情况主要是近年投标人在工程建设过程中因违反有关工程建设的法律、法规、规章或强制性标准和执业行为规范，经县级以上建设行政主管部门或其委托的执法监督机构查实和行政处罚，形成的不良行为记录。

2、合同履行情况主要是投标人近年所承接工程和已竣工工程是否按合同约定的工期、质量、安全等履行合同义务，对未竣工工程合同履行情况还应重点说明非不可抗力解除合同（如果有)的原因等具体情况，等等。

**（七）其他资格审查资料**

## 八、招标品牌要求及投标品牌反馈表

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **材料名称** | **招标品牌要求** | | **投标品牌** | **备注** |
| 信息系统安全等级保护测评 |  | |  | 符合资质要求的测评机构 |
| 供配电监测系统 |  | |  |  |
| 准入控制系统 |  | |  |  |
| 机房新风系统 |  | |  |  |
| 数据库审计系统 |  | |  |  |
| 桌管系统 |  | |  |  |
| 数据备份软件 |  | |  |  |
| 信息系统安全等级保护测评 |  | |  |  |
|  | | **备注：**  **1、报价清单须注明各设备的品牌及其规格型号。**  **2、所列品牌以参照目前市场占有率排名靠前品牌作为优先选用的参考，如有质量上同等及更优品牌，需具有权威机构提供市场占有率排名相关证明文件及投标产品在本地有具备完善的售后服务能力。** | | |

## 九、项目团队到岗履职承诺书

致柘城中医院有限公司有限公司（发包人）：

我单位参与投标的 项目，投标项目班子主要人员分别为：

项目经理：（本人签字）

实施人员：（本人签字）

实施人员：（本人签字）

我单位承诺：以上项目班子成员承诺均为本人签字，若中标，保证按上述人员依法进场履职（不可抗力除外），否则，愿意接受发包人依照合同进行处罚，以及建设行政主管部门依法处罚。

若非本人签字或未依法进场履职，违规（失信）单位及人员愿意接受一年内不得在全省范围内参加投标的处罚；失信人员停止一年执业资格；单位及个人记不良记录一次。

投标单位： （公章）

法定代表人： （盖章）

年 月 日

注：投标单位按要求填写，原件两份，投标人证件原件内一份、投标文件正本内一份（副本可用复印件）。

## 十、柘城中医院新冠肺炎疫情防控承诺书

为积极响应党中央、国务院以及省、市和县委县政府关于新型冠状病毒感染的肺炎疫情防控工作部署，确保个人和其他人员的生命健康安全，全面打赢疫情防控狙击战，结合医院实际情况，我本人（单位）作出如下慎重承诺：

一、自2022年以来，14天以内疫区及疫点接触情况说明：

是否从外省回来：是 🞎 否 🞎

若是，乘坐交通工具说明：

是否到过疫区：是 🞎 否 🞎

是否接触疫点：是 🞎 否 🞎

是否接触确诊或疑似患者：是 🞎 否 🞎

1. 自2022年以来，14天以内本人身体健康状况说明：

是否发热：是 🞎 否 🞎

是否咳嗽：是 🞎 否 🞎

1. 自2022年以来，14天以内本人是否被采取过集中隔离观察：是 🞎 否 🞎

如是，集中隔离 是 🞎 否 🞎 居家隔离 是 🞎 否 🞎

1. 本人（单位）承诺：在新冠肺炎疫情防控期间，自愿服从医院工作安排，不聚集，不外出，发现问题及时上报。若因本人提供的信息不真实或者不服从医院工作安排，所造成的一切后果由本人（单位）自行承担，

承诺人（签字，加盖公章）：

身份证号码：

联系电话：

现居住地：

2022年 月 日