合同编号：2025-162-XX

# 新疆医科大学第五附属医院网络机房系统及安全运维服务项目

# 合 同 书

项目名称：新疆医科大学第五附属医院网络机房系统及安全运维服务项目

服务地点：新疆医科大学第五附属医院

甲　　方：新疆医科大学第五附属医院

乙　　方：新疆惠文网络信息系统工程有限公司

签订日期：2025 年 6 月

# 合同细则

甲、乙双方在平等自愿、互惠互利的基础上，就甲方委托乙方对新疆医科大学第五附属医院网络机房系统及安全运维服务项目提供有偿技术服务事项，依据《中华人民共和国民法典》的相关法律、法规，双方同意按下述条款和条件签署本合同书（以下简称“合同”）并共同遵守。

## 1. 合同介绍

### 1.1. 甲方

| | | | |
|---|---|---|---|
| 甲方名称 | 新疆医科大学第五附属医院 | | |
| 通信地址 | 乌鲁木齐河南西路 118 号 | | |
| 联系人 | 吴鹏 | 手机 | 13369623089 |
| 电话、传真 | / | | |
| E-Mail | / | | |

### 1.2. 乙方

| | | | |
|---|---|---|---|
| 乙方名称 | 新疆惠文网络信息系统工程有限公司 | | |
| 通信地址 | 新疆乌鲁木齐市沙依巴克区黄浦江街 85 号和合苑小区 1 号楼 113 号 | | |
| 联系人 | 张新芳 | 手机 | 15022982017 |
| 电话、传真 | 0991-5565400、0991-5567739 | | |
| E-Mail | zhangxf@xjhw.net | | |

## 2. 服务内容

为甲方“新疆医科大学第五附属医院网络机房系统及安全运维服务项目”相关的网络运维服务、服务器存储与虚拟化平台运维服务、数据库运维服务、桌面运维服务、数据安全服务、机房动力环境运维服务、信息点部署服务、网络安全、互联网安全托管服务(含工具)、院内现有阳途终端安全管理系统和 TanCloud 监控系统扩容授权点及质保服务、提供运维 IT 综合运监控平台一套（服务器、网络设备、安全设备、存储、虚拟化平台等）。

### 2.1. 网络运维

#### 2.1.1 故障诊断及故障排除技术支持服务

在收到故障通知后，驻场工程师进行现场故障诊断及现场故障排除，直至故障确定或故障排除。出具故障报告，内容包括故障现象、故障原因、故障解决方法、故障处理建议等。需要更换配件或整机的情况，保修期内的设备协助联系厂家报修并跟踪厂家维修流程，直至故障排除；保修期以外的设备，配件由医院方另行采购，到位后再更换故障件，直至故障排除。

### 2.1.2 定期巡检服务

为医院方提供每月一次巡检服务，获得设备运行的最新资料，在院方同意后及时升级设备及系统的微码、补丁、特征库，同时第一时间发现存在的隐患，保障设备稳定运行。并有针对性地提出预警及解决建议，能够提早预防，最大限度降低运营风险。巡检为每季度提交设备巡检报告。

### 2.1.3 网络优化服务

网络优化服务主要内容是针对医院方网络，对其基础架构、网络性能、高实时性业务部署以及网络安全各方面进行评估、优化设计以及改进。此服务是建立在对医院方 IP 网络、业务构成进行充分调研评估的基础上，根据院方计算机网络容量和流量的要求，结合医院方需求，对医院方网络以及业务部署进行优化设计和实施，以提高网络可管理性、可维护性、安全性以及业务部署能力。网络优化服务为 4 次。

### 2.1.4 方案论证咨询服务

医院方网络正处于不断建设，不断发展的时期，包含广域网建设、局域网建设、网络安全建设等，在建设前期，方案是否可行，能否符合医院方的技术目标，是否存在潜在的技术隐患以及如何预防。网络方案验收服务在网络的规划设计阶段提供的一项专业服务解决方案。该服务通过对网络方案进行技术分析、仿真测试等，验证网络方案在技术方面的可行性、能否符合技术目标、是否存在潜在的技术隐患以及如何预防等。可以通过此项服务充分预防设备投资风险及网络运行风险，确保网络投资的有效与增值。方案论证咨询服务步骤：

1）验证规划设计

在提出网络方案验证需求后，乙方网络专家根据提供的网络规划方案中的内容，与医院方共同制定详细的网络验证方案，其中包括但不限于以下内容：

网络验证目标和验收标准

所要进行验证的内容

网络设备、仪器和所需的其他资源

验证项目的时间计划

所有确定的内容均直接体现在乙方网络专家拟定的《网络方案验证测试报告》中，并由医院方签字确认，作为此项服务的验收标准。

2）仿真与测试

乙方网络专家根据方案需求按比例搭建仿真网络环境，搭建所需设备由医院方提供，乙方并根据《网络方案验证测试报告》中所列测试项对网络性能和技术指标进行测试，其中包括但不限于以下测试内容：

验证规划方案的正确性和可行性

测试网络的冗余及可靠性

测试网络的整体性能及网络瓶颈点

测试网络其他技术目标

3）验证结果分析

在仿真网络环境测试完成后，乙方网络专家根据测试数据对网络方案进行整体分析，并将最终分析结果形成《网络方案验证分析报告》。该报告包括但不限于以下项目的分析结果：

验证该设计方案是否符合技术目标

证明该设计方案是否为最优设计方案

验证网络协议选择及设备选型是否正确

《网络方案验证分析报告》是此项服务最终输出结果，由医院方与乙方共同签字确认。

## 2.2.服务器、存储及虚拟化运维

### 2.2.1 工程师驻场服务

提供工程师现场驻场服务，随时解决医院方网络中出现的各类问题；驻场工程师熟悉医院方服务器、存储及虚拟化情况,具备服务器、存储及虚拟化工程师认证，有 3 年以上工作经验。

### 2.2.2 定期巡检服务

定期巡检为每周一次，对机房内的服务器和存储系统进行检查，分为硬件巡检和应用系统巡检。

1）硬件巡检

硬件巡检包括对服务器、存储系统的指示灯状态、部件工作状况、网络线路连接等情况进行常规巡检，主要检查是否有部件出现故障或可能出现故障，并对设备进行故障前检查。对故障前和故障的设备配件进行及时更换。更换配件如需停止运行相关设备需与医院方负责人沟通设备停机时间。设备在医院方要求的时间内完成故障配件的更换并保障医院方相关系统的正常运行。

在巡检过程中如设备配件出现故障乙方会对故障配件做如下处理：

质保内设备：如设备配件发生故障该设备在厂商质保期内乙方会与原厂商售后服务机构联系配合原厂商售后服务人员对设备做相关检测并与医院方协调设备是否需要停机及停机时间以配合原厂商售后服务人员更换相关故障配件，保障设备的正常运行；

质保外设备：设备已达到原厂商质保年限，乙方工程师在巡检过程中如果发现设备配件发生故障乙方工程师将启用备品备件机制通过乙方的备品备件库对故障配件进行更换，费用由乙方承担。更换配件时乙方与医院方负责人沟通配件更换时间及设备停机时间，以保障医院方业务的正常运行；

2）应用系统巡检

应用系统巡检包括对服务器、存储系统的操作系统状况、CPU 运行状态、内存占用情况、硬盘空间等，主要检查操作系统及存储系统的工作情况，排除已出现的系统故障或系统应用隐患，及时升级系统、打补丁、更新病毒库。如服务器操作系统出现故障乙方负责人有义务协助医院方对服务器操作系统进行重新安装（在重新安装操作系统前协助医院方对该服务器上的数据进行备份，乙方安装操作系统时在医院方要求的时间内安装相关服务器的操作系统）

3）巡检服务流程

乙方每周在提供服务前，提前与医院方进行确认，经医院方同意进入医院方的机房提供巡检服务，对设备的运行状态及故障指示进行做健康检查，为巡检结果出具巡检报告，每月出具一次巡检报告，并以巡检报告为医院方对乙方工作的验收依据。

### 2.2.3 设备维护服务

设备维护服务是每月 1 次巡检，对机柜线路的整理、设备标签检查更换、设备定期除尘、机房设备安装建议等服务。对进入医院方机房的新设备新线缆提供安装

建议，为设备的安装、调试，线缆的铺设、连接提供便利。对巡检时发现的故障，或突发故障进行排除。

### 2.2.4 备品备件服务

出现突发性的故障，会影响到医院的系统应用，因此需要在短时间内排除故障，恢复系统应用，而一些突发性故障很难短时间内进行排除，因此出现难以恢复的故障时，可利用备品备件服务进行恢复，乙方可在 4 小时内采用本地备件将故障恢复。乙方会在本地建立备品备件库，存放常用的服务器及存储配件，在相应设备出现故障后可及时更换。具体的备品备件清单见合同附件一。

### 2.2.3 数据库运维

#### 2.2.3.1 系统优化服务

随着应用系统投入使用时间的加长，系统由于数据量的增加或医院方数量的增加或应用的修改等各种原因导致的性能下降。性能降低后导致应用响应慢、统计或报表计算时间加长和难于维护等不良影响，严重影响生产效率。乙方利用各种工具手段跟踪系统现状，分析应用类型和医院方行为、评价参数设置、数据分布、硬件和系统资源的使用情况等，并提出相关调整建议，必要时可以随时在规定的时间内派技术专家到达医院方现场，处理医院方系统性能问题，确保医院方系统的高效运转。主要内容:与医院方共同制定性能调整范围文档；性能检查初始化参数调整；补丁或版本的改变；查找占用资源严重的 SQL 语句并提供优化建议；查找锁竞争并确保数据库运行效率；查找占用资源严重的进程；找出主要的性能瓶颈并及时解决；乙方工程师提供性能调整报告，包括相关发现及/或对结果的分析等内容。对于系统优化中发现的问题将持续跟踪并最终解决。

在单维度优化服务后，同时确保系统硬件资源充足，软件配置合理的情况下，医院方感知系统运行缓慢或当系统出现性能问题时，根据医院方的需要，以优化医院方体验为目的，在预定时间内对系统、数据库群集运行效率进行分析和调优，发现、定位和及时解决医院方体验不佳的可能问题点，全面提升业务系统医院方体验。综合调优服务主要内容：（服务内容包括）：各功能模块性能问题收集记录，并进行性能情况验证采集；对各项需要优化的操作从业务层，应用层，系统层进行逐层优化分析；操作实现业务逻辑分析；操作实现技术手段分析；应用程序数据访问特点分析；应用技术框架分析；操作实现底层代码分析；对后台系统环境进行优化分析；对各业务场景各操作涉及 SQL 语句进行优化分析；对涉及各数据模型进行优化分析；数据库表数据分布分析；数据空间数据存储方式分析；系统数据增长、数据

访问特点、空间需求分析与评估；应用布署方式分析优化；系统软件配置参数分析优化；系统软件版本及补充分析优化；根据优化分析情况，制定优化方案；跟进并执行优化测试；进行优化验证；制定正式生产环境优化布署方案；执行正式生产环境优化实施；正式生产环境优化效果验证提交成果；为最终医院方提供了本工作单元的内容并由获医院方认可；将根据医院方要求指定乙方工程师在双方约定时间内提供不间断的性能调优服务，每次优化须达到医院方提出的量化目标。

#### 2.2.3.2 紧急救援服务

1）在出现影响生产的严重故障时，二线专家团队成员能在30分钟之内响应，提出合理的处置建议，并在要求时间到达现场，快速进行系统恢复。系统恢复后分析故障原因，并提交报告。

2）在出现数据库损坏或数据丢失时，在没有备份的情况下或备份不完整不可用情况下能够使用特殊的数据恢复软件来最大限度地恢复数据。乙方所使用的特殊数据恢复软件有取得软件著作权并在业界有成功的应用案例。

3）在出现复杂、重大、疑难故障时，乙方能够组织经验和技术能够胜任的二线专家团队进行故障会诊，提出故障处理方案。

#### 2.2.3.3 关键业务时点驻场提供保障服务

1）对系统进行全面深度的健康检查，及时定位系统的安全隐患，并针对可能出现的故障隐患提出相应的修复方案和应急措施。

2）积极主动检查、监控系统的运行状态，及时发现问题、提前预防问题，对于可能影响系统的重大性能问题，及时沟通、主动推动问题的落实和处理，在部分问题原因不完全确定，没有解决方案时，主动提供有效的临时规避方案，使系统能够稳定地运行。

3）进行系统检查和风险管理，分系统进行架构、健康状态、安全状态、日志状态、备份等检查。

4）梳理业务系统存在的各种风险，划分风险等级，并针对存在的风险制订解决方案。

5）进行系统风险评估，基于对系统的日常监控及以往相关故障的原因分析，梳理目前系统中存在的风险。

6）根据系统运行情况进行系统支撑能力评估，按系统分别梳理清单列表和配置情况，对资源使用和能力进行评估。

7）根据专家深度健康检查结果和系统风险评估制定系统隐患修复方案，与医院方相关负责人讨论确定实施计划，并完成实施或制定应急预案。

8）对于已发现的需要从应用开发方面解决的软硬件架构问题，乙方可积极配合开发商制定修复计划或应急方案，确保在保障前排除隐患。

9）根据系统运行情况制订完善的应急流程、方案，并配合完成保障前重要系统的应急演练。

10）保障期间针对系统相关的各个关键环节制定全面的监控和性能数据统计方案，不断收集和分析监控和性能数据变化趋势，及时发现数据库相关的性能隐患，确保保障期间的性能稳定。

11）保障期间持续跟踪、分析数据库相关系统的负载峰值，落实优化调整措施，提高系统性能、确保系统的稳定运行。

12）保障结束后3个工作日内，主管部门和维护单位书面提交详细的《运行情况报告》，报告中包括业务承载情况、主要性能指标、数据库运行情况分析等。

#### 2.2.3.4 工程割接配合工作

对于重大的工程割接，为确保工程割接的顺利进行，乙方可组织技术专家配合工程的各项工作，主要包括工作：

1）组织技术专家参与整体方案讨论，并制订专门保障措施或方案。

2）工程割接前的各项准备工作，包括技术支持、系统环境准备、系统环境调整、SQL脚本审核、导入导出相关数据以及系统调优等。

3）配合相关厂商进行系统总体联调功能测试、压力测试。

4）进行测试环境搭建、数据准备、跟踪监控、结果分析、测试后环境清理。

5）组织或配合进行系统应急演练测试和网络、主机、数据库、中间件、应用程序系统故障切换测试。

6）在系统正式割接前的数据模拟割接中负责环境搭建、跟进处理模拟割接过程中发现的问题，并提出解决方案，并按要求改进实施。

7）割接期间安排工程师到现场全程跟进工程割接上线全过程，从环境的检查、安装、调试、部署、调优全程技术支持，随时应对突发事件发生,直至系统成功上线。

8）工程割接完成后，适时总结，提供分析报告。

9）割接完成后，配合医院方进行系统升级完成后的测试、提交系统割接实施报告和性能测试报告等。

### 2.2.3.5 应用版本上线配合服务

随着业务需求的日趋复杂，为避免版本上线对现网系统造成稳定性以及性能的影响，乙方可组织技术专家做好版本上线保障工作，包括：

1）为减少版本上线后出现的性能问题，争取在上线前尽可能地发现新版本中潜在的风险，并解决这些潜在性能瓶颈，进一步提升上线版本的质量，乙方从当前的数据结构及数据量情况出发，对开发商工程师提供的上线相关表结构、SQL 语句信息进行评估。

2）针对库表结构而言，从新增库表可能的数据量和未来维护效率、当前已存在的索引、索引冗余等多方面考虑其合理性。

3）SQL 语句的评审则主要是通过查看在测试环境中的执行计划，考察其是否有精简的可能性，是否合理使用现有索引，是否需要重构查询结构、改变访问顺序、添加适当提示等。尽可能减少 SQL 执行中的物理读、cpu time 等。针对优化空间较小的 SQL，及时与开发工程师联系，协商能否对应用层做一定修改。

4）组织工程师对版本上线的整个过程进行监控，从性能测试中及时发现上线后可能出现的性能瓶颈，并做出针对性的优化调整。

上线后，对系统进行强化的实时监控，及时发现新版本对系统的影响，配合处理版本上线后的性能等问题。

### 2.2.3.6 数据库监控服务

数据库监控服务，需要对数据库进行每日巡检，包括所有各类数据库。数据库日巡检内容如下：

1）核查所有实例运行 每日巡检

2）核查 LISTENER 正常运行 每日巡检

3）核查可以成功连接数据库 每日巡检

4）核查可以成功备份数据库 每日巡检

5）核查存储资源有充足的可用空间 每日巡检

6）查看日志文件中出现的任何错误 每日巡检

7）查看 SQL*Net 日志中的错误信息 每日巡检

8）检查数据库进程数量 每日巡检

9）检查会话(Session)锁状态 每日巡检

10）检查不可用索引(UnusableIndex) 每日巡检

11）管理FlashbackRecovery区(10g、11g) 每日巡检

12）查看CPU、内存、网络、磁盘的争用情况 每日巡检

13）检查定义在DBMS_JOBS/DBMS_SCHEDULER的JOB状态 每日巡检

14）识别空间受限对象(Space-BoundObjects) 每日巡检

15）检查分析性能数据Workload profile\Database Hit Ratios（数据库命中率）\TOP SQLs 每日巡检

#### 2.2.3.7 咨询和技术支援服务

1）提供咨询和培训服务：

根据医院方IT系统演进的规划，按医院方要求，不定期在数据库云化、整合、分布式数据库、Weblogic中间件等方面，提供电话、web、现场会议等手段的技术咨询；乙方在服务期限内提供至少5天的培训服务，每次参加培训的人数由医院方确定。每年提供1-2名相关专业认证的培训。

2）提供技术支援服务：

利用各种工具进行数据库性能监控，并通过各种手段不定期根据系统运行情况开展有效的优化。

### 2.2.4 桌面运维

对医院全部的内外网计算机的桌面操作系统运行维护，内容包括桌面终端操作系统的问题处理、重新安装，日常应用软件、业务系统应用软件的安装维护。

#### 2.2.4.1 台式机、笔记本、一体机、查询机等终端维护

1）院内电脑软硬件的日常维护、定期巡检、配件更换或增加、升级改造、故障诊断、故障排除、操作系统及应用软件升级，安装，以确保院内计算机系统正常使用（在维修维护过程中，工程师确保文件不丢失。系统无法修复需重装时，询问需保留的文件内容并进行备份。）。

2）设备故障鉴定、设备及配件提供更换建议、故障配件更换，定期清洁及预防性维护。

3）对院方新设备检测、现场安装调试；设备接入、设备迁移所需前端跳线、弱电井、小机房交换机到办公PC两端的网络跳线乙方提前准备；设备使用地点变更，按照院方要求负责设备拆卸、搬迁，新使用地点设备安装、调试、网络接入。

4）各种办公软件(OFFICE、WPS等)的安装、升级、参数配置，安装杀毒软件，定期进行杀毒，性能调试、故障排除等；

5）局域网连接，网络调整、共享资料等建立台账、并按季度巡检全院终端，提交巡检报告。

6）关键业务时间节点、重大系统割接、迁移以及上线配合服务提供保障服务。

#### 2.2.4.2 医院配置的扫描仪、刷卡器、PDA等设备

1)协助解决安装、调试扫描仪、刷卡器、PDA等外设。

2)软硬件的日常维护、定期巡检、配件更换或增加、升级改造。确保设备的正常运行。

3)定期进行性能调试、故障排除等;建立台账，定期更新维护台账。

### 2.2.5 数据安全运维

#### 2.2.5.1 数据安全服务

1)定期硬盘及存储介质底层检测，每季度不少于1次

2)硬盘健康状况检测报告

3)告知医院数据安全风险，提供解决方案及建议

4)重要数据及数据库进行定期备份安全测试，保证备份数据有效性

#### 2.2.5.2 紧急救援服务

维保内设备如遇任何数据安全故障，在备份不可用情况下提供上门数据恢复服务，最短时间内免费进行数据恢复工作，最大限度地恢复数据。具备以下数据灾难应急救援能力：

1)具有专业数据恢复人员,取得数据恢复工程师认证证书

2)在乌鲁木齐本地具备数据恢复所需条件，包括：独立的数据恢复工作间、数据恢复硬件设备、数据恢复软件

3)具有独立完成的磁盘整列和虚拟化环境下数据恢复相关案例。

### 2.2.6 机房动力环境运维

采用全包价的承包方式，维修保养费用包括：机房设备日常维护所需所有耗材、上下水管线、空调室外机清洗、更换原厂滤网、制冷剂、保险丝（管）等耗材，机房设备的维护、维修产生的材料费、故障维修所需的备件费、维修备件的运输费、搬运费、工程师及原厂工程技术人员的差旅费、维修费等全部费用。

机房动力环境运维服务内容包括每月一次现场巡检，以及机房设备日常运行维护，具体内容如下：

### 2.2.6.1 机房空调系统

1） 控制系统的维护

从空调系统的显示屏上检查空调系统的各项功能及参数；

如有报警的情况要检查报警记录，并分析报警原因；

检查温度、湿度传感器的工作状态；

2）压缩机的巡回检查及维护

检查压缩机工作状态，检查高、低压保护开关、干燥过滤器等其他附件。

3）冷凝器的巡回检查及维护

检查冷凝器的固定情况，冷凝器的固定件是否有松动的迹象，以免对冷媒管线及室外机造成损坏。检查冷媒管线有无破损的情况，检查冷媒管线的保温状况。检查风扇的运行状况：主要检查风扇的轴承、底座、电机等的工作情况，在风扇运行时是否有异常震动，风扇的扇在转动时是否在同一个平面上。检查冷凝器下面是否有杂物影响风道的畅通，从而影响冷凝器的冷凝效果；检查冷凝器的翅片有无破损的状况。检查冷凝器工作时的电流，从工作电流进一步判断风扇的工作情况。检查调速开关，检查在规定的压力范围内，调速开关能否正常控制风扇的启动和停止。

4）蒸发器、膨胀阀的巡回检查及维护

蒸发器、膨胀阀的维护主要是检查蒸发器盘管是否清洁，是否有结霜的现象出现，以及蒸发器排水托盘排水是否畅通。

5）加湿系统的巡检及维护

（1）观察水槽内是否有沉淀物质。

（2）检查上水和排水电磁阀的工作情况。

（3）检查加湿水槽排水管道是否畅通。

（4）检查漏水探测器。

6）空气循环系统的巡回检查及维护

（1）检查空调过滤器是否干净。

（2）检查风机的运行状况：检查风机各部件的紧固情况及平衡，检查轴承、皮带、共振等情况，皮带调整的松紧程度是否合适。

（3）测量电机运转电流，看是否在规定的范围内，根据测得的参数判断电机是否是正常运转。

（4）检查隔风栅。

（5）检查计算机及其它需要制冷的设备进风侧的风压。

### 2.2.6.2 机房UPS供电系统

1） UPS除尘处理

半年内对每台UPS进行一次除尘处理，详细检修实施步骤：中心机房有两台UPS，在除尘时可停掉其中一台，负载由另一台承担（需要评估负载承担风险），其他机房的单UPS只能停机处理。停机后打开UPS顶盖和UPS前挡板，用专用毛刷将电路板和重要部件的灰尘进行清扫，再用小风量专用小型吸尘器将浮尘吸净，对所有接线端子进行全面检查，检查有无发热现象，并做紧丝处理，以保证UPS所有接线完好，无松动。清扫和检修完毕后，开启UPS，检查UPS运行状态以及供电是否正常恢复。

按以上方法将所有机房的UPS清理干净并检修，需要专业工程师参加。

2） UPS风机检查

风扇在UPS各部件中占有非常重要的地位，一旦风扇出了故障，则整台机器将因过温而停止工作。因此，每次对UPS维护时将对风扇进行细致检查，一旦有风扇运行不正常或发出异常杂音，要及时更换。

3） UPS状态信息参数查询

在每次UPS维护时，先对UPS参数及信息进行查询，重要查询历史事件记录，看是否有告警代码，事件发生的日期与时间，查明原因并及时解决。如果是某控制部分参数或元器件有问题造成参数变化的告警，要更换此电路板，以确保UPS的安全工作。如果是市电或其他原因造成的告警且不影响UPS的正常使用的，要以书面形式加以说明。更改参数的及时更改，避免不必要的告警打扰。

4） UPS逆变器电容维护保养

对逆变器电容进行全面保养。每季度对逆变器电容进行一次放电激活，每台UPS将放电20分钟。每一年对逆变器电容做深度放电一次，已达到全面激活逆变器电容的目的，每台UPS放电40分钟。

5） 备用易损件

为了能做到突发事件的应急处理，在机房存放2套UPS主机的易损件（同型号旁路保险丝和逆变器电容直流保险丝）。并培训医院一旦出现应急情况应如何进行更换此配件和应注意事项。

### 2.2.6.3 机房动力环境监控系统

1） 软件部分

（1）检查服务器操作系统是否正常工作；

（2）检查服务器内硬件资源使用情况；

（3）检查软件是否正常使用；

（4）检查监控界面数据是否显示正常；

（5）检查监控界面内的报警数据、历史数据、系统日志等信息，对相关设备的故障及报警等信息及时处理；

（6）检查监控界面系统各项设置是否正常；

（7）通过修改报警阀值测试报警，查看短信、电话语音报警是否工作正常；报警接收人是否能正常接收报警信息；

（8）检查数据采集程序（监控状态）是否工作正常；串口程序、短信程序、电话语音程序、网络采集程序工作是否正常；

2） 硬件部分

（1）查看服务器硬件运行状态；

（2）查看数据采集板卡工作状态；

（3）查看前端温湿度、漏水等传感器是否正常工作；

（4）查看前端硬件通讯线是否有损坏或者松动的情况；

（5）测试前端部件灵敏度和精准度；

### 2.2.7 信息点部署服务

根据医院网络信息点部署实际需要，在运维服务期内，本项目包含每年100个六类网络信息点的零散布线服务，超出100个信息点的费用按照500元/个计算。

布线标准严格按照国家相关标准和规范，包含材料和人工。乙方在收到通知后，最晚第二天进场开工，完工后由医院方组织验收，以实际满足使用为准。

### 2.2.8 网络安全运维服务

根据医院的要求提供的网络安全技术服务，包括:医院安全设备系统安全配置的日常检查;协助配合做好网络安全检查、应用系统安全审计、安全应急管理等安全专项工作;终端安全管理各项工作;各类网络安全管理及安全支撑软件日常维护工作，协助医院对新采购安全设备集成方案审核，结合医院信息化实际情况提出安全设备配置及规划合理性建议。为了能够更好的体现运维服务的能力，网络安全运维服务报告结合综合运维平台提供响应运维报告。

一、固定性工作(驻场人员完成)

1）日常安全巡检：定期对安全设备进行巡检，出具报告，结合医院现有安全手段，发现的信息安全事件，及时通知并协助相关责任方进行处理。 1次/日

2）安全预警：定期以邮件或内部沟通工具的形式向医院通告安全态势，重要系统漏洞及补丁版本信息等。不定期将网络安全相关事件及紧急重大漏洞信息，以最直接的方式向医院告知其安全隐患、影响范围及补救措施等。服务频率：36次/年

3）重大安全保障：在节假日期间或重大活动期间对于网络安全事件的监控、响应与处置。服务频率：根据需求

4）安全集成审核：协助医院对新采购安全设备集成方案审核，结合医院信息化实际情况提出安全设备配置及规划合理性建议。服务频率：根据需求

5）日常安全事件分析：对安全事件进行及时发现并处置，如WEB漏洞攻击，恶意扫描，恶意IP装库，SQL注入，CVE漏洞利用等恶意攻击。服务频率：根据需求

6）驻场服务：提供1名安全服务人员驻场服务，服务期一年。

二、周期性工作（二线人员完成）

1）安全培训服务：定期针对不同医院类型，设计有针对性的安全培训内容，组织有经验丰富的讲师授课，提升网络安全意识。

服务内容包含但不限于安全意识培训、安全开发培训、安全测试培训、安全技能培训和高级安全管理培训。服务频率：1 次/年

2）应急响应：当安全事件发生时，可以由专业的服务团队协助其分析判断事件因果、降低损失、提供有效的问题解决建议。高级服务人员根据事件类别，通过远程和现场支持的方式协助客户对遇到的突发性安全事件进行紧急分析和处理。主要工作内容包括：突发事件信息收集、事件分析、分析报告提交、问题解决建议等。根据实际需求配合上级单位或牵头组织应急演练服务，定制应急演练剧本，搭建应急演练环境，形成应急演练文档。服务频率：1 次/年

(1)定期检查医院数据中心机房、安全设备的管理、策略配置；完成安全设备、网络设备的日常安全巡检工作；对院方终端安全管理系统、网络日志审计系统等关键安全设备的技术维护工作。

(2)乙方提供网络安全应急响应管理服务，完成重大安全事件的应急响应工作，出现网络安全事件能协调各个厂家进行事件处理，以及业务恢复等工作。

(3)在服务期内配合政府和行业主管部门的安全攻防演练工作，提供互联网及内网的安全渗透测试防守方服务，制定防守方案，协助院方协调安全厂商协助，使医院系统顺利通过检查。

(4)各类应用系统的日常安全事件监控、安全事件管理、网络安全预警等工作；结合医院现有安全手段，发现的信息安全事件，及时通知并协助相关责任方进行处理。收集业务安全需求，制定并优化安全分析规则与策略，不断完善优化各类安全策略。

(5)乙方协助医院方对院方网络安全系统整体建设、规划、建设规范、制度规范及相关标准进行制定，形成标准化文档，同时协助医院方对院方网络安全建设提出相关安全建设需求。

(6)乙方协助完成院方内部的网络安全检查工作，并对检查结果协助进行整改，同时按要求完成院方网络安全自查工作，整理相关材料，提供自查报告。

(7)对主机和应用系统进行漏洞扫描工作，针对威胁漏洞编写整改方案进行整改；完成主机、网络等安全基线检查等检测工作，同时提供基线合规加固指导服务；完成主机、网络漏洞下发工作，同时监督、跟踪漏洞处置情况。

(8)协助新业务系统上线，在新业务系统上线前进行网络安全配置检查、安全策略调整，提出新业务部署的相关安全建议。

(9)完成每年度的信息安全相关培训，包含但不限于：信息安全意识教育、设备操作、安全加固指导等。

(10)结合院方内部网络整体安全，发生病毒大面积爆发时，完成及时隔离操作，完成病毒分析工作，编写手工处置病毒文档。协调桌面终端安全厂商，给出病毒解决方案，预防病毒再次爆发。

(11)重要节点或节假日对网络安全应急保障值守工作。

(12)配合各个厂商做好设备巡检，维护的协调工作。

(13)配合做好重要节点的安全防护工作，除项目服务团队外，应增派资深专家团队现场支持做好安全防护工作。

(14)合同有效期内免费提供专业综合运维软件一套，监控防护院方所有网络设备、安全设备、服务器、虚拟化平台等。详细参数见合同附件三。

### 2.2.9 安全托管服务

合同有效期内免费针对院方DMZ区及互联网出口提供安全托管服务。乙方需借助第三方安全厂家设备为医院方搭建云网端安全运营平台和安全专家团体共同构建7*24小时持续守护、有效预防和主动闭环的体系化安全运营能力并提供保险服务。

为了能够更好的提升医院方的安全服务能力，需在医院互联网及DMZ区业务主机部署终端探针，网络侧部署流量探针，从而更全面的建立围绕资产、漏洞、威胁、事件四个风险要素的手段监测医院网络安全态势。

（1）服务上线

组件部署与接入：安全专家对需要接入MSS的组件（如TSS/SIP/AF/EDR等）进行部署并接入至MSSP安全运营平台。

资产收集与录入：安全专家在上线前对服务资产进行收集，并将资产信息录入到安全运营平台中进行管理。

（2）安全现状评估

策略检查：上线前安全专家对安全组件上的安全策略进行统一检查，确保安全组件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。

脆弱性评估：对操作系统、数据库、常见应用/协议、系统与Web漏洞进行漏洞扫描，弱口令扫描可实现信息化资产不同应用弱口令猜解检测，如：SMB、Mssql、Mysql、Oracle、smtp、VNC、ftp、telnet、ssh、mysql、tomcat等。

资产暴露面梳理：安全专家在上线前使用扫描组件对资产开展暴露面探测，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协助处置，实现对暴露面资产可管可控，降低暴露面资产的风险。（本项服务根据客户实际业务情况按需提供）

（3）安全问题处置

策略调优：安全专家根据安全威胁/事件分析的结果以及处置方式，对安全组件上的安全策略进行调整工作。

脆弱性问题修复指导：针对内网脆弱性，安全专家分析研判后提供实际佐证材料，并给出修复建。

（4）服务交付物：

《项目启动会PPT》、《首次安全风险分析报告》、《漏洞举证报告》（按需）

《漏洞清单》（按需）、《应急响应报告》（按需）、《威胁情报》、《暴露面梳理清单》(按需)、《威胁狩猎报告》（按需）、《安全运营周报》、《安全运营月报》、《半年度总结汇报》、《年度总结汇报》

### 2.2.10 现有运维管服务

对医院现有的阳途终端安全管理系统和TanCloud监控系统做日常运行维护服务，包括新需求的响应、授权扩容、版本升级等服务。

## 3. 服务方式

常驻服务：乙方派出 三 名系统维护工程师常驻甲方，负责日常运维服务有关事项。

## 4. 服务期限

4.1. 服务期限为两年，合同一年一签；本合同约定的服务期从2025年6月21日起，至2026年6月20日止。

## 5. 合同金额及支付方式

5.1. 本合同期限为 壹 年，合同总金额为：人民币 572,800.00 元（大写：伍拾柒万贰仟捌佰元整），以上合同价格包括维护服务、税费、人工、设施设备、调试、调试等全部费用，甲方除支付合同约定的上述款项外，无需再支付其他任何费用及款项。

5.2. 支付方式：

5.2.1. 合同签订后按每三个月进行一次考核，付款依据三个月一次的运维服务工作评价结果而定；

5.2.2. 每三个月一次的评价结果为合格的情况下，支付年度合同总价款的 25%,即人民币 143,200.00 元（大写：壹拾肆万叁仟贰佰元整）。

5.2.3. 若评价结果不合格，甲方有权拒绝支付任何费用，且甲方有权限期乙方进行整改，直至评价合格。

5.3. 银行账户信息：

5.3.1. 甲方信息：

开户银行：交通银行股份有限公司乌鲁木齐开发区支行

户　　名：新疆医科大学第五附属医院

账　　号：651100860018000820993

地　　址：乌鲁木齐市新市区河南西路 118 号

电　　话：7598428,7598425

5.3.2. 乙方信息：

开户银行：中国工商银行股份有限公司乌鲁木齐明德路支行

户　　名：新疆惠文网络信息系统工程有限公司

账　　号：3002010119200033118

地　　址：新疆乌鲁木齐市沙依巴克区黄浦江街 85 号和合苑小区 1 号楼 113 号

电　　话：0991-5565897

甲方向以上账户付款，即为完成本合同项下对乙方相应的付款义务。乙方对提供账户信息的准确性和可用性承担全部责任。若以下账户状态或信息发生任何变更，乙方应提前7个工作日使甲方获悉，否则甲方不对乙方迟延收到或未能收到任何款项承担责任

5.4. 甲方向乙方支付每笔款项前，乙方向甲方提供符合财务做账要求的对应金额的发票（票种：增值税普通发票，税率：6%，品名：技术服务费），否则甲方有权拒绝支付任何价款并且不承担任何违约责任。

注：合同金额仅为合同中约定的服务内容，不包含超出合同约定的软件升级、更换硬件、硬件维修产生的费用。

## 6. 双方的权利与义务

6.1. 乙方为确保提供优质服务，在甲方服务点安排服务工程师负责技术服务工作,并保持必要的补充技术力量。乙方可根据甲方要求及时更换服务工程师。

6.2. 甲方应为乙方人员提供必要便利的工作环境。乙方工程师因工作需要可以检查、维护甲方系统涉及的相关计算机设备及其资料文档。对甲方应用环境的较大调整，须由甲方人员主持实施。

6.3. 乙方人员需严格遵守甲方有关制度，按照合同约定项实施技术服务。

6.4. 甲方按约定支付乙方合同金额。

6.5. 甲方从乙方购置、维修合同约定外的计算机耗材、配件、其他软硬件等，乙方承诺提供优质服务和合理价格；协商价格后双方另行签订补充协议。

## 7. 甲方验收计划

7.1. 根据服务质量，甲方部门负责人每三个月对乙方进行一次考核，填写维保/售后服务考核表。维保/售后服务考核表一式肆份，甲乙双方各持所需份数。

7.2. 一年考核四次，合同签订后按每三个月进行一次考核，付款依据三个月一次的运维服务工作评价结果而定；每三个月一次的评价结果为合格（80分及以上）的情况下，支付年度合同总价款的25%,；若评价结果不合格，限期进行整改，直至评价合格。最终的服务质量验收以全年四份维保/售后服务考核表为准。全年考核

服务分 80 以上，按合同规定支付。全年考核服务分 80 以下，扣除合同总价款 20%作为违约金。

7.3. 合同签订后甲方对乙方每三个月进行一次考核作为付款依据，并依据一年四次考核结果决定是否签订第二年度服务合同。

## 8. 禁止转包服务

8.1. 在本合同有效期内，乙方必须亲自履行甲方委托的服务内容，未征得甲方的书面同意，不得将其在本合同项下的服务项目部分或全部转让给任何其它方执行。

## 9. 保密条款

9.1. 乙方应对甲方系统环境、设备的技术资料和技术秘密采取保密措施，乙方未经甲方的书面同意，不得将本项目所涉及的技术秘密和资料向与本项目无关的人员或第三方透露，也不能就有关合同内容的任何部分进行新闻的发布、公开的宣称、否认或承认。否则承担由此产生的经济上和法律上的责任。

9.2. 在本合同项目结束后，乙方应向甲方提供本合同项目的所有相关文档。乙方应归还甲方提供的所有技术资料或文件等，并承诺不保留任何复印件。

9.3. 乙方在下列情况下没有为任何信息保守秘密的义务，即当该信息已为公众所知且不是由乙方未经授权而提供时；当该信息是由乙方从第三方合法地接受该信息且没有保密限制时。

9.4. 本条规定的义务和权利在本合同期满或终止后将持续叁年有效。

## 10. 知识产权

10.1. 乙方承诺，其在受托服务本合同项目中，不侵犯或非法使用第三方的知识产权。乙方有权利拒绝甲方的侵犯或非法使用第三方的知识产权的建议或要求。

10.2. 任何因甲方原因而引起对第三方知识产权的侵权诉讼，乙方应当积极协助甲方进行抗辩。

## 11. 不可抗力

11.1. 不可抗力是指本合同生效后，发生不能预见并且对其发生和后果不能防止或避免的事件，如地震、台风、水灾、火灾、战争等，致使直接影响本合同的履行或不能按约定的条件履行。

11.2. 发生不可抗力的一方应立即通知对方，并在十五天内提供不可抗力的详情及将有关证明文件送交对方。

11.3. 发生不可抗力事件时，甲乙双方应协商以寻找一个合理的解决方法，并尽一切努力减轻不可抗力产生的后果。

11.4. 如不可抗力事件持续三十天时，甲乙双方应友好协商解决本合同是否继续履行或终止的问题。

## 12. 违约责任

12.1. 任何一方不履行或不完全履行本合同约定义务的，应当承担相应的违约责任，并赔偿由此给守约方造成的损失，包括但不限于守约方为实现债权而支付的律师费、保全费、诉讼收费、公证费、鉴定费等；

12.2. 若乙方未按合同约定履行服务，每逾期一日，应向甲方支付合同总额的1‰的违约金，乙方逾期付款累计超过30日时，甲方有权解除本合同，由此给甲方造成损失的，乙方应承担赔偿责任。解除合同并不影响乙方对上述违约金的支付。

12.3. 若甲方未按本合同约定付款，每逾期一日，应向乙方支付合同总额按中国人民银行定期存款利率的违约金。

12.4. 由乙方造成的重大事故,乙方应承担相应的责任。重大事故包括但不限于因程序修改、增加引起的程序错误，系统发生故障并造成宕机未在限定时间内解决的。因乙方责任造成系统重大事故的，处置完后应填写重大事故表。

## 13. 解除合同

13.1. 一方严重违反本合同项下的义务，另一方应当以书面形式告知违约方纠正行为，违约方在收到对方通知后三十天内仍未纠正，守约方有权单方解除本合同，本合同在解除通知书到达违约方时解除。如果该违约行为无法在三十天内纠正，而违约方在此期限内已经开始着手，并将以努力诚恳继续纠正此违约行为，则守约方应为违约方合理地延长该时间的期限。

13.2. 当本合同以任何原因终止时，乙方应立即停止使用并销毁包含甲方机密信息的所有物件，并证明该销毁情况；或者将这些物件归还对方。

## 14. 争议解决

14.1. 履行本合同过程中发生争议，双方应友好协商解决，经协商仍不能解决的，任何一方均可向甲方所在地法院提交诉讼仲裁。

## 15. 一般条款

15.1. 除非本合同另有规定，任何一方对本合同提出的任何弃权、修改或更改须以书面形式提交给对方，并经对方签字认可，否则本合同的任何条款均不得视作已被弃权、修改或更改。本合同的修改或变更，须由双方友好协商并经授权代表签署书面文件方可生效。

15.2. 合同各方在此声明并保证：（1）代表各方签署本合同的人员拥有明确的授权，其签字对签约方具有约束力；（2）本合同的执行、递交与履行不会违反各方公司的章程、规定；（3）本合同的执行、递交与履行已经得到全部所需合作方或公司行为的正式授权；并且本合同已对上述方形成了有效的、具有约束力的同时能按其条款执行的义务。

15.3. 本合同与附件、相关招投标文件构成双方间的完整的合同，并将取代之前所有的书面或口头、执行或未执行的讨论、合同或声明。未经双方授权代表再签订正式合同，本合同将不作变化、增删和修改或其他活动。

## 16. 合同生效

16.1. 本合同一式<u>陆</u>份，由甲方执<u>肆</u>份、乙方执<u>贰</u>份，具有同等法律效力。自合同双方授权代表签字并加盖公章之日起生效。

**（以下无正文，为签字盖章处）**

| | | | |
|---|---|---|---|
| 甲方（盖章）： | 新疆医科大学第五附属医院 | 乙方（盖章）： | 新疆惠文网络信息系统工程有限公司 |
| 法定代表人： | 史秋银 | 法定代表人： | 董斌 |
| 甲方代表： | 吴鹏 | 乙方代表： | 张新芳 |
| 联系人： | 吴鹏 | 联系人： | 张新芳 |
| 联系电话： | 13369623089 | 联系电话： | 15022982017 |
| 甲方确认司法送达地址： | 乌鲁木齐高新区（新市区）河南西路 118 号 | 乙方确认司法送达地址： | 新疆乌鲁木齐市沙依巴克区黄浦江街 85 号和合苑小区 1 号楼 113 号 |
| 开户行： | 交通银行股份有限公司乌鲁木齐开发区支行 | 开户行： | 中国工商银行股份有限公司乌鲁木齐明德路支行 |
| 账号： | 651100860018000820993 | 账号： | 3002010119200033118 |
| 签订日期： | 2025.6.20 | 签订日期： | 2025.6.20 |

## 附件一：备品备件清单

| 序号 | 品牌 | 型号 | 配件 | 数量 |
|---|---|---|---|---|
| 1 | 宝德 | PR2012P3 | 电源 | 3 |
| 2 | 宝德 | PR2012P3 | 风扇 | 6 |
| 3 | 华为 | 2288HV5 | 电源 | 16 |
| 4 | 华为 | 2288HV5 | 风扇 | 16 |
| 5 | 联想 | SR860 | 电源 | 2 |
| 6 | 联想 | SR860 | 风扇 | 4 |
| 7 | H3C | R4900 | 电源 | 4 |
| 8 | H3C | R4900 | 风扇 | 4 |
| 9 | IBM | P730 | 电源 | 2 |
| 10 | IBM | P730 | 风扇 | 2 |
| 11 | IBM | P740 | 电源 | 2 |
| 12 | IBM | P740 | 风扇 | 2 |
| 13 | EMC | VNX5400 | 电源 | 2 |
| 14 | EMC | VNX5400 | 风扇 | 2 |
| 15 | EMC | VNX5400 | 硬盘 | 4 |
| 16 | EMC | VNX5600 | 电源 | 2 |
| 17 | EMC | VNX5600 | 风扇 | 2 |
| 18 | EMC | VNX5600 | 硬盘 | 4 |

| 序号 | 品牌 | 型号 | 配件 | 数量 |
|---|---|---|---|---|
| 19 | 华为 | OceanStor 5310 | 电源 | 1 |
| 20 | 华为 | OceanStor 5310 | 风扇 | 1 |
| 21 | 华为 | OceanStor 5310 | 硬盘 | 2 |
| 22 | 华为 | OceanStor 5130F V5 | 电源 | 1 |
| 23 | 华为 | OceanStor 5130F V5 | 风扇 | 1 |
| 24 | 华为 | OceanStor 5130F V5 | 硬盘 | 2 |
| 25 | 华为 | OceanStor 5110 | 电源 | 1 |
| 26 | 华为 | OceanStor 5110 | 风扇 | 1 |
| 27 | 华为 | OceanStor 5110 | 硬盘 | 2 |
| 28 | 华为 | OceanStor 5310F V5 | 电源 | 3 |
| 29 | 华为 | OceanStor 5310F V5 | 风扇 | 3 |
| 30 | 华为 | OceanStor 5310F V5 | 硬盘 | 6 |

## 附件二：专业综合运维软件一套

| 模块 | 功能项 | 功能描述 |
| --- | --- | --- |
| 整体架构 | 运行环境 | 1、全中文界面B/S架构；可支持Linux操作系统及国产操作系统平台下部署。 |
| | | 2、提供大屏数据展示，提供两种大屏风格界面供使用人员选择。 |
| | | 3、支持登录访问控制自定义限制IP登录功能。 |
| | | 4、支持系统登录密码复杂度安全设置符合等保要求 |
| | 系统架构 | 1、支持自身服务监控当服务异常时，可以发送告警给相关运维人员。 |
| | | 2、支持自定义修改IP地址功能，系统管理页面修改IP |
| | | 3、支持日志管理历史数据自定义保留时间，减少大量系统日志占用存储 |
| | | 4、支持日志管理历史数据保留期限，可以通过文本的形式查看历史数据。 |
| 综合监控 | 操作系统监控 | 1、支持对CPU利用率，CPU负载的监控，反映CPU的使用和消耗情况。可以配置CPU持续时间段占用率超过一定数值进行告警，例如“持续10分钟CPU使用率超过90%”。 |
| | | 2、支持对磁盘剩余空间，磁盘IO的监控。可以配置存储空间占用率达到一定数据进行告警，当存储空间不足时会产生告警，例如“服务器192.168.1.100上C盘分区磁盘空间使用率高于99%”。 |

| | | |
|---|---|---|
| | | 3、支对内存使用情况监控。 |
| | | 4、支持对网络负载、网卡流量进行监控。例如当上行或者下行带宽达到一定数据进行告警。 |
| | | 5、支持线型统计图展示历史监测点数据趋势，提供近半小时、近三小时、今天以及近三天数据查询 |
| | | 6、支持对操作系统的状态进行，当发生重启或者不可访问时，会发生告警进行。例如“服务器 192.168.1.100 刚才发生重启”，“服务器 192.168.1.100 失联，持续 3 分钟未响应”。 |
| | | 7、支持监测点数值、IP、设备名称排序，便于运维人员即使发现处理 |
| | **数据库监控** | 1、支持 MySQL/SQL Server /postgresql/GBase/SyBase/redis/Oracle/DB2/MongoDB/Cach é 和国产数据库达梦/金仓的监控。 |
| | | 2、支持连接数等各类性能指标的监控。 |
| | | 3、支持死锁等高可用指标的监控。 |
| | | 4、支持每秒提交事务/每秒回滚事务/每秒已连接数量/每秒读字节等操作指标操作 |
| | | 5、提供对每秒读写速度、已连接数量、执行语句数、IO 操作、CUP 解析花费、提交事务监测点以线型统计图展示数据趋势。 |
| | | 6、支持对数据库监测点告警记录并显示告警时长以及告警恢复时间 |

| | | |
|---|---|---|
| | | 7、数据库密码凭证统一加密存储，后续便于添加设备添加 |
| | 中间件监控 | 1、支持对 Nginx、JVM、Tomcat、WebLogic、WebSphere、docker 等中间件的监控，主流的中间件都支持。 |
| | | 2、支持对 ActiveMQ、RocketMQ、Kafka、IBM、WebSpher、Jboss、minio、canal 华为 FusionInsightrabbit、rabbitMQ 等消息队列的监控。 |
| | | 3、支持对中间件如 docker 镜像个数、连接状态、容器运行状态以及内存最大值、cup 使用率、内存使用率等实时监控，及时响应告警运维人员 |
| | | 4.支持接入中间件获取版本信息数据、运行时间的显示 |
| | 网络设备监控 | 1、支持对不同品牌网络设备的自动发现、自动生成拓扑图功能。 |
| | | 2、支持交换机断路报警，网络拓扑展示交换机的链路情况，绿色表示连通正常，红色表示断路，系统能够进行及时报警。 |
| | | 3、支持可视化展示不同品牌交换机端口开关状态 |
| | | 4、支持显示不同交换机品牌、型号、运行时间、描述信息 |
| | | 5、支持显示交换机下 VLAN 对应 IP 信息以及 IP 地址表、转发表、路由表、ARP 表信息。 |
| | | 6、支持针对不同交换机端口输入/输出流量、交换机内存、CPU 使用率的监控 |
| | | 7、支持对不同品牌交换机接口流量监控、发送/接收数据包流 |

| | | |
|---|---|---|
| | | 量数据、广播包、丢包率功能。 |
| | | 8、支持对不同交换机监测点阈值自定义编辑，提供不通颜色区分告警等级设定 |
| | | 9、支持针对交换机 snmp 密码凭证加密统一存储管理，减少交换机凭证重复输入 |
| | | 10、支持交换机监测点历史告警记录显示，提供告警连续时长以及告警回复时间显示 |
| | | 11、支持图形化界面展示交换机监测点异常点 |
| | | 12、支持线型统计图形式展示近半小时、近三小时等流量、内存使用率、CPU 使用率趋势 |
| | | 13、支持交换机网络拓扑监测点连线异常的颜色变化 |
| | | 14、支持交换机实时告警数据统一显示管理，可对告警详细信息确认和查看 |
| | | 15、支持大屏展示交换机监测点 TOP 数据，实时滚动展示监测点历史告警数据，以及告警恢复数据 |
| | | 16、支持针对交换机监测点提供配置企业微信、钉钉、邮箱、短信形式实时发送告警通知 |
| | | 17、支持交换机端口状态连续告警时长自定义天数忽略告警功能 |
| | | 18、支持不同交换机网络拓扑中创建子拓扑以及分组管理 |
| | | 19、支持交换机在网络拓扑中物理链路的统一管理，实时展示 |

| | | |
|---|---|---|
| | | 端口状态、链路状态等 |
| | | 20、支持提供不同交换机接入可根据设备名称、IP 等信息筛选查找 |
| | | 21、支持不同品牌交换机接入，可根据 IP、设备名称、CPU 使用率以及内存使用率进行排序展示 |
| | | 22、支持对不同交换机新建自动发现任务，可设置执行周期、发现 IP 范围 |
| | **服务器监控** | 1、支持对华为、戴尔、华三、惠普、联想、浪潮、HP UX、IBM AIX、Linux、Windows 各品牌物理服务器的监控。 |
| | | 2、支持对跨平台(Windows、Linux、Unix) 操作系统级指标项的监控。 |
| | | 3、支持读取服务器处理器、内存、硬盘等的配置信息。 |
| | | 4、支持对服务器历史监测点数据图形化界面展示，针对流量等数据采用线型统计图展示数据趋势 |
| | **存储监控** | 1、支持对惠普、日立、EMC、群晖、IBM、戴尔、华为、H3C、中科曙光、等各平台物理存储设备的监控。 |
| | | 2、支持磁盘大小读取、磁盘温度、磁盘坏扇区数、系统温度以及 RAID 可用大小和 RAID 热备盘数等监控 |
| | | 3、支持读取服务器的网口状态、速率、以及流量等信息。 |
| | | 4、支持自定义阈值告警监测点颜色区分 |
| | **虚拟化** | 1、支持对 vmware、华为、华三、深信服思科、京东云等厂商 |

| | | |
|---|---|---|
| | | 的虚拟化平台的监控，包含对主机资源池情况的监测，包含主机 cpu、存储、内存等资源的分配情况。同时可查询到主机下子机的运行情况，包含状态、资源使用率能性能指标。 |
| | | 2、支持虚拟机磁盘空间大小监控、磁盘剩余空间监控、内存使用率、以及内存剩余空间等监控 |
| 拓扑展示 | 业务服务 | 1、支持查看当前业务的总体运行状态，业务下监控结点最大的 CPU、内存、磁盘等使用率。 |
| | | 2、支持业务拓扑图，支持查看业务下的告警情况，支持查看业务下单个监控主机的运行情况，点击能够打开监控详情。 |
| | 网络拓扑 | 1、基于 H5 技术实现拓扑图功能，通过拓扑图模块用户能了解当前生产网络的整体运行情况（如本视图上设备的统计、性能、异常，网络流量等），能自动生成真实物理拓扑图。 |
| | | 2、链路支持实线和虚线，支持链路流动，可根据链路的流量大小支持不同颜色、颜色可以调色面板的方式用户自定义。 |
| | | 3、拓扑图支持分组。支持鼠标放大和缩小拓扑图。 |
| | | 4. 支持网络拓扑链路一键管理，便于运维人员查看 |
| | | 5. 支持链路故障时颜色呈现红色线条状态，故障恢复时及时响应由红色线条变更成绿色线条 |
| 监控告警 | 实时告警 | 1、支持实时告警的统计。 |
| | | 2、支持实时告警按照严重程度分类排序。 |
| | | 3、支持告警等级颜色区分 |

| | | |
|---|---|---|
| | | 4、支持告警等级颜色以图形化界面统计展示 |
| | 告警配置 | 1、支持短信、邮件、钉钉、企业微信、微信公众号等各种通知媒介的方式进行告警，无需二次开发支持。 |
| | | 2、支持各类媒介消息模版的配置。 |
| | | 3、支持指定时间类故障未恢复将向领导推送。 |
| | | 4、支持消息的订阅，按照监控对象、故障等级分发给不同的运维人员。 |
| | | 5、支持灵活的报警策略配置管理和灵活的报警忽略功能。 |
| 统计报警 | 日报周报 | 1、支持自动生成报警信息的日报、月报分析统计和导出功能。 |
| | | 2、支持对物理资产、虚拟资产、业务资产进行分类统计， 支持台账导出。 |
| | | 3、支持对网络流量、内存、CPU 等各类的 Top 排行和查询功能。 |
| | | 4、支持自定义报表设备类型显示 |
| | 流量报表 | 1、支持整个系统接入设备所产生监测点数据进行排序，针对输出输入流量进行统计 |
| | | 2、支持对服务器 CPU、内存周平均峰值的统计分析。 |
| | | 3、支持对单台设备报警、资源分配、性能三线图、报警环比对照信息查看。 |
| | | 4、支持对运行一段时间的业务系统生成健康度报告，含报警、资源分析等。 |

| | | |
|---|---|---|
| | | 5、支持一键导出表格流量报表文档 |
| | 实时报表 | 1、支持对当前未恢复报警的分类查询统计功能。 |
| | | 2、支持对历史报警的分类查询统计功能。 |
| | | 3、支持对一段时间报警的分类统计功能。 |
| | | 4、支持自定义新建报表统计，可自定义设备类型生成报表 |
| | TOPN 报表 | 1. 支持系统接入设备 TOP 监测点排序并一键导出生成报表 |
| | | 2. 支持自定义设备类型 TOP 监测点展示 |
| | 监控大屏 | 1、通过已纳入管理的 IT 资源告警情况、关键指标等，平台创新性的设计了运维驾驶舱大屏功能，可实时界面展示监控整体运行情况。 |
| | | 2、支持自定义监控大屏设计，可以将关键业务或者核心系统的监控情况进行展示。 |
| 系统设置 | 组织架构 | 1、支持建立三权管理，区分管理员、普通用户、以及子管理员，同时支持自定义角色自定义列表便于后续管理 |
| | 用户管理 | 1、展示用户列表，包括姓名、登录账号、所处部门、手机号码等，可以按照用户名进行查询，也可对用户信息进行增加、修改、删除以及给用户关联对应角色。 |
| | 角色管理 | 1、展示角色列表，包括角色名称、角色描述等，可以按照角色名称进行查询，也可对角色信息进行增加、修改、删除以及给角色关联对应资源菜单 |
| | 日志审计 | 1、支持日志管理记录智能运维管理平台用户操作记录，包括 |

| | | |
|---|---|---|
| | | 登录、添加数据、修改数据、退出等操作 |
| | **系统登录设置** | 1、支持用户登录首次登录修改密码、密码超过天数强制提示修改、以及系统登录过期时间、登录失败次数锁定账号、 |
| | **密码复杂度** | 1、支持密码复杂度设定，密码格式长度以及格式要求 |

附件三：入场报告

| | |
|---|---|
| 甲方 | 新疆医科大学第五附属医院 |
| 乙方 | 新疆惠文网络信息系统工程有限公司 |
| 合同号 | 2025-162-XX |
| 项目名称 | 新疆医科大学第五附属医院网络机房系统及安全运维服务项目 |
| 入场时间 | |
| 项目入场说明 | |
| 根据项目前期调研、方案规划，双方依据形成的《项目准备工作清单》开展准备工作，目前项目准备工作关键事项已完成，具备入场实施条件，现正式入场实施，予以确认。<br>项目入场后项目组成员依据项目工作职责及实施计划，密切配合开展项目工作，确保项目按计划完成。 | |
| 甲方代表签字<br><br>年　月　日 | 乙方代表签字<br><br>年　月　日 |

## 附件四：维保/售后服务考核表

_____年____月_____项目

使用科室：　　科室签字：

| 考核项目 | 考核要素 | 考核要素定义 | 评分 |
| --- | --- | --- | --- |
| 服务能力（60分） | 处置问题/故障响应时间（0-10分） | 是否满足合同约定响应时间，不满足一次扣5分 | |
| | 处置问题/故障时间（0-10分） | 是否满足合同约定处置时间，不满足一次扣5分 | |
| | 服务窗口覆盖（0-10分） | 是否提供7×24小时支持（节假日含），不满足扣5分 | |
| | 处置问题/故障解决率（0-10分） | 首次修复后又重复修复，重复修复一次扣2分 | |
| | 预防性维护（0-10分） | 是否按计划执行定期巡检、设备保养、系统优化等，四次以上满分，少一次扣2.5分 | |
| | 技术文档提交（0-10分） | 是否提交维修报告、巡检记录、维保记录等文件， | |

| | | | |
|---|---|---|---|
| | | 不满足一次扣 10 分。 | |
| 服务满意度（40） | 投诉次数（0-10 分） | 投诉 1 次扣 5 分 | |
| | 不良事件（0-10 分） | 不良事件一次扣 5 分 | |
| | 沟通主动性（0-10 分） | 是否及时通报故障进展、提供解决方案建议，不满足一次扣 5 分 | |
| | 用户满意度（0-10 分） | 科室人员对服务态度、沟通效果的评分， | |
| 总分 | | | |