# 诸葛运帷 IT 运维监控系统运维服务参数

## 一、维保服务范围

服务期内，服务提供方需对医院 IT 运维监控相关资源进行全面纳管、深度监控与全生命周期管理，确保运维系统有效支撑医院 IT 业务稳定运行，具体纳管与监控范围包括但不限于：

1.IT 业务系统：医院核心业务系统及非核心业务系统的运行状态、业务流程衔接、异常告警等；

2.服务器设备：涵盖 Windows Server、Linux（含 CentOS、RedHat 等主流版本）等操作系统的物理服务器与云服务器，监控指标包括 CPU 使用率、内存占用率、磁盘 I/O、网络吞吐量、进程状态等；

3.存储设备：SAN 存储、NAS 存储、对象存储等各类存储设备的存储空间利用率、读写速度、数据冗余状态、设备健康度等；

4.数据库系统：MySQL、Oracle、SQL Server 等主流数据库的连接数、查询响应时间、事务处理效率、数据一致性、日志完整性等；

5.中间件：Tomcat、Nginx、WebLogic 等中间件的服务启停状态、线程池占用率、请求处理量、错误日志等；

6.虚拟化平台：VMware、Hyper-V 等虚拟化平台的虚拟机运行状态、资源分配合理性、宿主机负载、虚拟网络连通性等。

## 二、维保服务要求

**（一）服务响应时效要求**

1.医院通过电话、书面信函、传真、指定邮箱等方式提出服务请求后，服务提供方需在1 小时内积极响应。

2.响应内容需包含但不限于：服务请求对应的问题初步分析结果（需结合医院 IT 系统架构与历史运维数据）、拟采取的处理方案方向（分远程协助、现场服务两类明确）、预计处理时长（精确到小时，需符合本文件后续故障恢复时限要求）、本次服务对接人姓名及联系方式（确保 7×24 小时可联络）。

**（二）现场服务与故障恢复要求**

故障等级界定：故障等级由医院根据业务影响范围与程度书面界定，服务提供方无异议，具体标准如下：
 一般故障：不影响医院核心业务系统运行，仅对非核心系统或局部功能有轻微影响。
 重大故障：影响医院核心业务系统正常运行，或导致多类 IT 资源同时中断，可能引发医疗服务秩序混乱。

**2.现场服务时限：**

一般故障：服务提供方确认需现场处理后，需在48 小时内（含节假日，以医院发出现场服务需求通知的时间为准）安排具备相应资质的技术人员到达医院指定地点；

重大故障：服务提供方确认需现场处理后，需在24 小时内（含节假日，以医院发出现场服务需求通知的时间为准）安排技术负责人到达医院指定地点。

**3.故障恢复时限与违约责任：**

若故障为运维系统许可软件自身问题（如软件 Bug、许可失效等），服务提供方需在到达现场后12 小时内恢复系统正常运行。

若故障为非许可软件问题，服务提供方需在到达现场后24 小时内恢复系统正常运行。
 若因服务提供方技术能力不足、响应延迟、资源调配不当等自身原因未能按时恢复，每延迟 1 小时，需按服务合同总金额的 0.5% 向医院支付违约金（累计违约金不超过合同总金额的 20%）；若延迟超过 48 小时导致医院医疗服务受严重影响，医院有权终止服务合同，并要求服务提供方赔偿实际经济损失。

**（三）安全自查与审计配合要求**

**1.安全自查配合：**服务期内，服务提供方需配合医院每半年开展 1 次系统安全自查；

自查内容需覆盖：运维系统及所纳管 IT 资源的日常运行稳定性（如是否存在频繁告警、资源占用异常波动）、系统漏洞（含软件已知漏洞、配置漏洞、权限漏洞）、安全策略有效性（如防火墙规则、入侵检测策略、数据备份策略）、病毒与恶意代码防护状态等；

自查完成后，服务提供方需在10 个工作日内协助医院出具《IT 系统安全自查报告》，报告需包含自查过程、发现问题清单（标注风险等级：高、中、低）、问题成因分析。

**2.安全审计配合：**

服务提供方需配合医院每半年开展 1 次安全审计（与安全自查同步进行），审计内容需覆盖：运维系统及所纳管 IT 资源的账号合规性（如是否存在冗余账号、过期账号、共享账号）、权限分配合理性（如是否存在越权访问权限、权限未及时回收）、操作行为日志完整性（如日志记录是否覆盖关键操作、日志保存时长是否符合法规要求）、安全技术措施有效性（如防火墙、杀毒软件、数据加密工具的运行状态与更新情况）；

审计过程中，服务提供方需按医院要求提供运维日志、系统配置文档、漏洞扫描报告、权限分配清单等资料（需在医院提出需求后 2 个工作日内提交）。

**3.隐患整改配合：**

对自查与审计中发现的安全隐患，服务提供方需在7 个工作日内协助医院制定可落地的整改方案（明确整改措施、责任人员、时间节点、验证标准）；

整改期间，服务提供方需每周向医院提交《隐患整改进展报告》，跟踪整改进度；整改完成后，需协助医院开展验证测试，确保隐患闭环处理（高风险隐患整改验证需在整改完成后 3 个工作日内完成，中、低风险隐患需在 7 个工作日内完成）。

**（四）保密要求**

1.服务提供方需在服务合同签订前，与医院签订保密协议。

2.保密范围包括但不限于：医院 IT 资源信息（服务器配置、存储架构、网络拓扑等）、业务数据（患者诊疗数据、收费数据、员工信息等）、系统配置信息（运维系统参数、账号密码、接口密钥等）、技术文档（运维方案、应急预案、自查报告等）、考核数据（服务质量评分、故障处理记录等）；

3.服务提供方需采取保密措施：建立内部保密管理制度，限制敏感信息的访问权限（仅授权参与本项目的技术人员接触），禁止以任何形式（纸质、电子、口头）向第三方泄露、篡改、滥用保密信息；若因服务提供方原因导致保密信息泄露或被滥用，服务提供方需承担全部法律责任（包括但不限于行政责任、刑事责任），赔偿医院因此造成的经济损失（含直接损失与间接损失），并立即采取补救措施（如删除泄露信息、加固系统防护）；

4.保密期限：服务提供方需持续履行保密义务。