

陆丰市第二人民医院信息系统及网络硬件 运维服务项目

用 户 需 求 书

陆丰市第二人民医院

2026 年 7 月

目 录

一、项目概况.....	3
1、项目背景.....	3
2、项目目标.....	3
二、项目内容范围.....	3
1、信息系统运维服务范围.....	3
2、硬件运维服务范围.....	5
三、主要商务要求.....	7
四、技术标准与要求.....	8
1、主要技术服务内容.....	8
2、应急响应服务.....	13
3、技术团队要求.....	15
4、保密要求.....	16
5、维护登记制度.....	16
6、项目风险管理.....	16
7、项目培训要求.....	17
8、文档交付要求.....	17

一、项目概况

1、项目背景

陆丰市第二人民医院经过前期建设，已经完成医院信息管理系统、数据机房建设，已形成医院 HIS 基础系统、电子病历系统、PACS 影像系统、LIS 检验系统、健康体检系统、传染病管理系统、临床路径管理系统、院感管理系统、医保控费系统、随访管理系统、手术麻醉管理系统、移动查房/护理系统、医务质控系统、数据分析管理系统等 14 个软件系统平台以及超融合平台、安全等保管理平台、灾备平台；16 台硬件服务器及内外网核心交换机等设备，基本涵盖医院外科、妇产科、内科、儿科、检验科、功能影像科等临床、医技与管理科室业务流程与管理流程。实现“以病人为中心”统一管理、互联互通、信息共享的“互联网+医疗”信息管理系统平台。

考虑医院业务的特殊性和复杂性，需确保系统和网络硬件等能高效、及时提供业务支撑。通过统一的智能运营平台实现主动信息系统运维服务模式，降低后台核心资源的故障率，并提升资源利用率，保障医院信息系统的高效；通过网络硬件安全运维服务模式，分析存在问题和短板，从运行维护规划、运行维护管理、运行维护实施、运行维护质量、运行维护安全、运行维护评估及持续改进等方面提出构建科学运维管理体系的建议措施，保障医院机房和网络安全高效的运行。因此，系统和网络硬件运行的稳定性、顺畅性至关重要。

2、项目目标

（1）信息系统运维服务目标

加强信息系统运行维护管理，维护系统正常运行、记录系统的运行情况；保证业务系统的正常运行，确保陆丰市第二人民医院日常业务、运营、管理等工作正常开展；建立一套规范、先进、安全、稳定的运维体系，最终达到提高服务满意度并降低成本的目的。

（2）网络硬件运维服务目标

保障陆丰市第二人民医院机房硬件和网络的正常运行，出现问题后能及时解决问题，保证陆丰市第二人民医院各项业务的开展。

二、项目内容范围

1、信息系统运维服务范围

陆丰市第二人民医院信息系统于 2022 年 3 月进入系统运维周期，运维服务项目截止至 2026 年 4 月到期，为医院系统对陆丰市第二人民医院业务系统的有力支撑。旨在不断完善和提升系统运维水平，确保信息系统安全可靠和稳定运行，提升信息化建设和服务的总体效能。主要信息系统运维服务范围如下（模块名称）：

序号	系统名称	模块名称
1	门诊信息系统	门诊预约挂号系统
		门诊分诊系统
		门诊收费系统
		门诊医生工作站
		门诊护士工作站

		门诊中西医药房系统
		门诊配液管理系统
	急诊信息系统	急诊预约挂号系统
		急诊分诊系统
		急诊收费系统
		急诊医生工作站
		急诊护士工作站
		急诊中西医药房系统
2	住院信息系统	急诊留观系统
		住院出入转系统
		住院收费系统
		住院医生工作站
		住院护士工作站
		住院中心药房系统
		住院配液中心系统
3	电子病历系统	会诊管理系统
		门急诊电子病历
		住院医生电子病历
4	移动医生工作站 移动护士工作站	病历质控系统
		移动医生工作站
		住院 PDA 护士执行
5	传染病管理 院内感染管理系统 临床路径管理系统 重点患者管理 死亡证明书管理 护理管理系统 危急值管理平台 随访系统	移动护理管理
		传染病管理
		院内感染管理系统
		临床路径管理系统
		重点患者管理
		死亡证明书管理
		护理管理系统
		危急值管理平台
6	随访系统	随访系统
		医学影像传输与归档系统 (PACS)
		医学影像传输与归档系统 (PACS)
7	实验室信息系统 (LIS)	实验室信息系统 (LIS)
		实验室信息系统 (LIS)
	手术麻醉系统	手术麻醉系统
		手术麻醉系统
7	体检系统	体检系统

8	综合查询系统	综合查询基础功能
		统计室统计系统
		院长查询
9	对外接口	新医保平台、国家医保 2.0 对接改造
		食源性报卡监测上报接口对接
		国家药品追溯产品功能改造接口
		广东省病案系统对接
		绩效考核与医疗质量管理住院病案首页采集系统对接
		医疗收费电子票据接口
		省内、省外异地门诊住院接口
		灵狐财务系统接口
		医保人脸识别、智能监管接口
		汕尾、陆丰区域平台数据上传接口
10	医保控费	国家传染病上报对接接口
		项目付费
		人次付费
11	其他	总额预付
		医院信息平台
		护理病历
		药库管理
		物资管理系统
		收费模块

2、硬件运维服务范围

根据项目服务目标及医院当前的现状，网络硬件运维服务范围，主要分为以下四个部分：

A. 加强机房、网络设备、网络安全管理：为保障信息化应用系统很多基础数据、业务平台都正常运行，网络安全成了重中之重，一旦机房或设备毁坏、数据写迷惑篡改将直接给单位带来巨大的损失，例如：机房着火、UPS 无法供电、重要系统遭到篡改等。

B. 加强应用系统监管和安全分析：在网络安全的基础上，医院工作逐步依赖软件系统，系统的运行稳定才能保障日常工作有序运作。

C. 持续保证核心硬件设备的维护工作：通过对应用系统和核心硬件设备投入必要的维护力量，更加全面专业的进行应用系统和核心硬件设备的保养、升级、巡查、维修等工作，保证网络基础环境稳定。

D. 对机房和网络进行日常巡检、维护，保障业务科室的正常使用。

以下为本次网络硬件运维服务范围如下：

序号	设备名称	品牌	型号	SN 码 (序列号)	数量	单位	备注
核心机房 (外网)							
1	数据库服务器 1	浪潮	NF5280M4	419163382	6	台	总线服务器
2	数据库服务器 2	浪潮	NF5280M4	419163391			hqms
3	数据库服务器 3	浪潮	NF5280M4	419163384			pacs db
4	数据库服务器 4	浪潮	NF5280M4	419163394			his db
5	数据库服务器 5	浪潮	NF5280M4	419163379			报表
6	数据库服务器 6	浪潮	NF5280M4	419283454			灵狐中间表
7	应用服务器 1	浪潮	NF5280M4	419163393	6	台	pacs 应用
8	应用服务器 2	浪潮	NF5280M4	419163380			测试
9	应用服务器 3	浪潮	NF5280M4	419163395			his ecp
10	应用服务器 4	浪潮	NF5280M4	419163396			his ecp
11	应用服务器 5	浪潮	NF5280M4	419163385			his ecp
12	应用服务器 6	浪潮	NF5280M4	419267728			一体机
13	备份服务器 1	浪潮	NF5280M4	419163388	2	台	Pacs mirror
14	备份服务器 2	浪潮	NF5280M4	419163392			his mirror
15	存储设备 1	浪潮	AS2150G2	218686518	2	台	
16	存储设备 2	浪潮	AS2150G2	218686519			
17	光纤交换机 1	锐捷	RG-S5750C-28SFP4XS -H		2	台	
18	光纤交换机 2	锐捷	RG-S5750C-28SFP4XS -H				
19	核心交换机 1	锐捷	RG-S6220-48XS4QXS		4	台	
20	核心交换机 2	锐捷	RG-S6220-48XS4QXS				
21	核心交换机 3	锐捷	RG-S6220-48XS4QXS				
22	核心交换机 4	锐捷	RG-S6220-48XS4QXS				
23	多业务路由器	锐捷	RG-RSR50-X-84		1	台	
24	超融合平台	深信服	计算服务器虚拟化软件 V5.0 超融合平台		1	套	
25	下一代防火墙	深信服	AF-1000-C600-QS	5058004059	1	套	
26	应用防火墙 (WAF)	深信服	WAF-1000-D420-S3	5017507792	1	套	
27	数据库审计系统	深信服	DAS-1000-A620-SK	5031021209	1	套	

28	入侵检测系统	深信服	NIPS-1000-A400-SK	5058002939	1	套	
29	灾备系统	深信服	aStor-EDS1210	9CC1000143	1	套	
核心机房（内网）							
30	核心交换机 1	华为			2	台	
31	核心交换机 2	华为					
32	防火墙	华为			1	台	
33	无线控制器(AC)	华为			1	台	
34	出口路由器	锐捷	RG-RSR50-X-84		1	台	
35	上网行为管理	深信服			1	套	

三、主要商务要求

序号	内容	要求
1	合同履行期限	自合同签订之日起 1 年
2	项目地点	陆丰市第二人民医院指定地点
3	付款方式	（1）预付款：合同签订生效后 10 个工作日内，采购人向成交供应商支付 2 个月的运维服务费用； （2）进度款：按月付款。采购人在每月 20 日前向成交供应商支付上月运维服务费用。当月度进度款累计支付满 8 个月运维费用后，采购人暂停支付月度进度款； （3）尾款：合同履行完毕 12 个月服务期且通过验收合格后 10 个工作日内，采购人一次性付清尾款。
4	验收要求	本项目质量必须符合国家、省、市及行业现行相关验收标准、验收规范与售后服务的要求，若未能达到该要求的，则不予以验收，并应对存在的质量缺陷问题及时整改。服务期满后，由运维单位撰写服务完成报告，由采购人委派的负责人在审核后签署。服务完成报告的签署，标志着服务项目通过验收。
5	履约保证金	不收取
6	报价要求	报价已包含系统维护费、网络硬件检查检测费、人工费、税费以及合同实施过程中不可预见费用等完成本项目内容所需的一切费用。更换配件、设备维修及购置软件系统的费用由采购人承担。
7	售后服务	提供 7*24 小时的售后服务热线
8	其他	本项目服务期限为 1 年（12 个月）。服务期内，如因医院信息系统升级替换、信息化建设任务取消、上级主管部门政策重大调整等情形，继续履行合同将损害公共利益的，采购人有权提前终止本合同。采购人应提前 30 日向成交供应商出具书面终止通知，合同终止后，双方按照供应商实际提供服务

		的时长据实结算服务费，互不承担违约责任。服务费按实际服务自然月折算结算，采购人仅支付已履约部分费用，无需支付剩余未履约周期服务费用。
--	--	--

四、技术标准与要求

1、主要技术服务内容

(1) 信息系统运维主要技术服务内容

a. 系统维护管理工作

制定和实施软件系统维护服务计划；定期提交维护报告，维护到期提交总结报告；安排业务经验丰富的设计人员进行问题处理方案的审核；根据用户的维护制度完成维护工作。

b. 系统改正性维护服务

当软件在特定情况下运行暴露出程序错误，必须在接收到问题后按服务级别规定时间对问题进行诊断和定位、进行程序修改、验证和补丁发布。

c. 系统完善性维护工作

纠正前台用户误操作。对因用户误操作导致某项业务不能办理完毕，或业务经办结果错误，在后台进行业务回退、业务结果修订；系统的日常维护，如故障排除、版本更新、日志清理、参数配置及其他相关工作。

d. 系统响应支持工作

系统故障诊断及检修：当系统出现故障时，必须及时对操作系统进行诊断、分析，并排除故障；成交供应商负责提供院方的本项目在维保期内的操作系统最新、稳定级别的升级版本，由院方根据应用现状自行决定是否安装使用该新版本。版本更新信息以设备原厂商官方网站公布为准；成交供应商协助院方进行操作系统和其承载的应用系统的重新安装、系统优化、操作系统（微码）版本升级、补丁安装、应用升级和调整等的方案设计、测试、现场实施等工作，并提供相关工作的详细技术文档。

信息系统运维服务内容响应表

服务项目	具体内容	时间/频率	响应级别
日常维护	1. 定期巡检所涉及软件系统工作状态 2. 定期对巡检记录和日志进行分析,发现各系统中存在的系统问题和隐患并及时处理 3. 对巡检服务进行记录,提交巡检服务记录; 4. 帮助解决运维中遇到的各类技术问题。	按不少于每月 12 个工作日	C
事件处理	1. 通知相关人员, 交换必要的信息; 2. 对现场作记录, 保护一切可作为证据的记录(包括系统时间、所采取行动、与外界沟通等等); 3. 采取措施, 尽量限制涉及的范围, 决策是否关闭系统、是否断开网络、是否监视系统等; 4. 解决问题、根除隐患, 充分理解导致事故发生的系统	按不少于每月 12 个工作日	A

服务项目	具体内容	时间/频率	响应级别
	脆弱点，并作补救措施，同时对事故进行备档； 5. 恢复系统，使系统运行正常； 6. 提交事故处理报告。		
分析报告	1. 软件系统巡检报告； 2. 软件系统服务报告；	按不少于每月 12 个工作日	B
服务可用性：7×24 小时内 99%可用（不包括计划停机时间）； 服务响应时间：10 分钟；			

（2）网络硬件运维主要技术服务内容

a. 机房动环系统维护服务

监测各级回路的开关状态；监测输入/输出电压、电流、频率、功率，蓄电池组的电压、后备时间、温度等参数，整流器、逆变器、电池、旁路、负载等部件的状态；监测电源防雷器的工作状态，对防雷器被雷击或浪涌破坏进行实时的记录和报警通知；监测输入市电状态，各部件的状态及参数，监测蓄电池组的电压、电流、温度、容量等参数。

定期巡检、测试，确保各个系统工作状态正常；建立完善应急制度，确保紧急情况下，损失将至最低；根据机房内设备数量情况，及时调整各个系统的负载能力，确保系统有效工作；定期审核各个系统工作日志，及时发现并排除隐患；定期梳理各个系统的工作逻辑，确保系统联动安全可靠。

机房动环巡检表单

检测地点	中心机房
功能检查	1) 监控系统软件维护
	☐ 检查组态软件是否运行正常，设备是否通讯正常；
	☐ 检查软件中的设备参数、状态是否正常；
	☐ 检查WEB端功能是否工作正常；
	☐ 检查远程控制功能是否正常；
	☐ 检查本地语音报警、电话报警功能是否正常；
	2) 监控系统主机维护
	☐ 检查CPU温度、主板温度是否异常；
	☐ 检查显卡、多串口卡、视频捕捉卡等板卡是否松动，散热片是否过热；
	☐ 检查鼠标是否能够滑动顺畅，无阻滞现象；
	☐ 检查主机多串口卡连接部分是否松动；
	☐ 清洗主机防尘滤网；
	3) UPS子系统维护
	☐ 检查各接线端子、通讯接口是否有松动现象；
	☐ 检查模块的电源指示灯、状态指示灯是否正常；

	☐ 检查UPS历史曲线趋势图，看电压、电流、有功功率等是否有异常波动，电池后备时间等是否在正常值范围内；		
	☐ 在条件允许的情况下，模拟UPS报警，检查监控系统是否正确报警；		
	4) 空调子系统维护		
	☐ 检查空调历史曲线趋势图，看温度、湿度等是否有异常波动，压缩机、风机工作时间等是否在正常值范围内；		
	☐ 在条件允许的情况下，模拟空调报警，检查监控系统是否正确报警；		
	5) 温湿度监测子系统维护		
	☐ 检查模块的电源指示灯、状态指示灯是否正常；		
	☐ 使用温度计测量实际温度，确认温湿度传感器是否需要校正；		
	☐ 检查温湿度传感器的历史曲线趋势图，看温度、湿度等是否有异常波动，并与空调的温湿度变化对照。		
	☐ 在条件允许的情况下，模拟温湿度报警，检查监控系统是否正确报警；		
其它			
检测结论			
检测人员		检测日期	
注：（√为合格，×为不合格，--为无此项）。			

b. 机房硬件设备维护服务

所有硬件设备保持整洁；硬件设备标签准确，与资产管理系统数据一致；定期巡检，硬件设备指示灯正常，所有变化记录在案；供电、数据、接地等线缆连接稳固安全；按设备预留冗余线缆，并确保线缆状态正常；设备工作温度正常，无水汽凝结；检测设备实际工作功率，确保供电满足。现有各类硬件设施，主要包括服务器、存储设备、网络设备、安全设备等，均在硬件服务范围内，需建立一套完整的硬件维护体系。

基础巡检内容表

检查项目	检查内容
IT 系统架构拓扑图	IT 系统架构拓扑图
网络设备配置	设备型号，IOS 版本，模块型号和数量,用途
存储系统配置	设备型号，IO 带宽，Cache 容量，磁盘数量，接入模式，存储容量，LUN 配置，所属应用
主机系统配置	设备型号，CPU 配置（类型，主频，数量），内存容量，网卡配置（数量，速率），内置硬盘配置（数量，容量，Raid），所属应用。

硬件环境巡检表

检查项目	描述	满足标准
------	----	------

检查项目	描述	满足标准
机房功能	服务于何种业务系统	N/A
温度	机房温度范围	摄氏 16-25 度
湿度	机房湿度范围	30%-55%
UPS 保护	稳压继电作用，是否部署	存在 UPS 设备，供电时间根据客户实际情况确定
防雷保护	是否存在	是
接地保护	是否存在	是
防静电保护	是否存在	是
地板承重能力	最大承重	800KG/平方米
防火设施	是否存在	是
防鼠设施	是否存在	是
门禁控制	是否存在	是
监视器	是否存在	是
卫生状况	环境清洁	是

设备运行状态检查表

检查项目	描述	满足标准
设备外观状况	无破损	是
设备状态灯	是否有告警灯闪亮	无
设备运转状况	功能正常	是
带宽利用率	是否在 80%以内	是
CPU 利用率	是否在 80%以内	是
日志系统是否有错误		无
线路冗余	冗余线路的负载能力要能够满足生产系统负载需求。	是
网络系统监控机制	是否存在	是

存储系统检查表

检查项目	描述	满足标准
设备外观状况	无破损	是
设备运转状况	功能正常	是
RAID 级别	根据业务类型和容错需求判断是否适合	是
Hot Spare	是否配置热备盘	是
硬件冗余配置	硬件是否存在单点故障	否
访问控制	是否配置访问控制	是

可用容量		20%以上
数据增长率	评估可用容量的可用时间	N/A
系统日志	是否有严重报错	无

主机系统检查表

检查项目	描述	满足标准
设备外观状况	无破损	是
设备运转状况	功能正常	是
硬件系统日志	是否有严重报错	无
网卡状态	可用	是
IP 地址配置		N/A
路由配置		N/A
网络联通状况	链路是否畅通	N/A
文件系统类型		N/A
分区剩余状况	是否存在即将写满的分区	无
分区合理性	Swap 分区达到物理内存的 2 倍;VAR 分区是否达到 2GB	是
外存储接入设备	设备型号	N/A
外存储接入设备速率	传输速率	N/A
RAID 级别	根据业务类型和容错需求判断是否适合	是
应用数据部署位置		N/A
CPU 负载情况	利用率小于 85%; 运行队列小于 CPU 个数的 4 倍, 阻塞队列小于运行队列; 交换队列为零; 互斥失速小于 CPU 个数的 250 倍。	是
CPU 配置信息	是否多个 CPU 全部用于处理	是
主要负载进程	是否存在再用系统资源过多的进程	否
内存使用情况	使用率低于 90%; 页面调出不持续增加; 不存在页面扫描活动	是
磁盘 IO 状况	是否存在 IO 热点	否
网络负载	平均利用率低于 80%	是
口令管理	密码复杂程度高: 长度超过 8 个字符; 设置为无意义字符组合; 多类型字符组合; 大小写混合组合。 定期修改, 强制口令过期。 限制口令重试次数。	是
系统补丁	更新为最新	是

病毒防范措施	安装病毒防火墙	是
系统日志	不存在验证错误警告	是
主机系统监控机制	是否存在	是

c. 安全检查支撑服务

高危端口排查：端口扫描的定义是客户端向一定范围的服务器端口发送对应请求，以此确认可使用的端口。虽然其本身并不是恶意的网络活动，但也是网络攻击者探测目标主机服务，以利用该服务的已知漏洞的重要手段。因此排查高危端口是整个安全体系建设中非常重要的一环，在发现高危端口时能够及时提醒安全、运维人员做出相应处理。本服务开展信息系统网络开放端口情况排查、梳理目前整体网络端口暴露面情况，重点针对勒索病毒常用端口（135、137、139、445、3389）。

弱口令检查：弱口令问题可谓是最常见、危害最大，也是最容易被利用的网络安全问题，各类信息系统中只要用到密码的地方就会有弱口令问题。本服务采用黑白盒测试方法，安全人员使用工具破解后与弱密码字典比对，对信息系统的操作系统密码、web 登录密码、数据库密码的进行弱密码检查。

安全配置核查：配置核查的核心价值是为了主动提前进行安全的弱点管理，通过配置核查减少攻击面，提高漏洞容忍度，提升防御强度，对基线合规检查、关键设备日志审计、网络关键区域安全审计和机房安全检查，依据设备的部署环境、承载业务等因素，核查是否满足基本安全配置要求的合计，并给出指导加固方案。

漏洞扫描服务：系统漏洞就是指系统本身出现极其严重的漏洞，这些漏洞很容易被病毒、木马、黑客等侵入，导致软件崩溃或者盗取重要信息、密码等。本服务主要是基于漏洞库进行网络扫描工作，包括 CGI 漏洞扫描、POP3 漏洞扫描、FTP 漏洞扫描、SSH 漏洞扫描、HTTP 漏洞扫描等内容，通过对主机（包括网络设备、数据库和中间件）和应用系统等对象进行安全扫描，发现其他安全隐患。

安全检查支撑服务表

序号	服务项	服务频率
1	高危端口排查	每半年一次
2	弱口令检查	每半年一次
3	安全配置核查	每半年一次
4	漏洞扫描	每半年一次
5	渗透测试	每半年一次
6	安全设备巡检	每半年一次

2、应急响应服务

（1）信息系统运维应急响应服务

① 提供 7×24 小时服务（每周 7 天，每天 24 小时响应服务，含所有国家规定的节假日）提供至少一名责任工程师的移动电话，7×24 小时响应服务请求。

② 在服务期间，运维服务商配备 1 名驻场维护工程师到医院值班备勤，提供每月不少于 12 个工作日每日 8 小时现场驻守服务。除现场驻守服务以外的时间段，对于紧急问题不能在远程处

理的，驻场维护工程师在 2 小时内到达现场处理。

③ 电话技术支持服务解答用户在系统使用中出现的問題。

④ 实时远程诊断服务。

⑤ 紧急上门服务。

⑥ 在非工作时间，包括节假日，妥善做好维护应急方案和值班安排，并将值班安排提前 2 小时书面告知用户方。所安排的值班人员应该具备一定的技术能力和应急处置能力，能够处理或者协助处理突发的系统事件。根据实际情况，可能需要在节假日期间安排维护服务人员到现场进行值班服务。

⑦ 购置软件系统的费用由采购人承担。

(2) 网络硬件运维应急响应服务

a. 响应处理计划

① 应能在 10 分钟内准确诊断并告知用户故障原因，诊断差错率要控制在 5%以内。并向最终用户解释故障发生原因，可能导致的后果，以及拟采取的措施。

② 故障修复过程中可能影响用户工作或系统应用数据有影响的，要先咨询用户意见再处理。

③ 如果配件需要送修或更换，维修期间提供同档次的备用设备，并需要配合单位用户登记故障配件的型号和产品序列号，并由用户签字后再送维修。

④ 如果机器送修，需要保护好磁盘等存储设备。要先将用户数据备份好，再送维修。

⑤ 建立巡检制度：所有设备进行月度的巡检检查，记录设备状况，列出注意事项，并反馈给用户。

⑥ 设备维修结束后，维修人员需向用户出示服务维修单。服务维修单上需注明维修日期、维修人员、维修地点、故障、故障原因分析、修复结果等。

⑦ 更换配件及设备维修的费用由采购人承担。

⑧ 服务类型要求：送修、现场、特殊服务要求（如购件、升级等）

⑨ 每月月度报告，每季度、年总结以及维护统计。

⑩ 现场运维确认表：工程师现场运维填写现场运维表，故障排除后由用户签名确认。

b. 响应处理时限

① 提供固定的 7×24 小时故障受理电话服务。

② 提供每月不低于 12 个工作日 8 小时驻场服务。达到 100%的用户响应度，（非工作时间或节假日提供热线或电话支持服务，如有需要，须提供现场服务）。

③ 技术人员响应时限：接障后技术支持人员即时响应，详细记录故障现象，并根据服务级别设定判定服务级别。

④ 到达现场时间：工作时间 30 分钟（一级）、非工作时间 1 小时（一级）。

⑤ 平均业务恢复时间：30 分钟（一级）。

⑥ 最大设备修复时间：3 个工作日。

⑦ 取回维修的设备维修周期为：三个工作日。

⑧ 重要设备在维修周期内必须提供相应的替代产品以保障网络及应用不会受到影响。

c. 服务级别设定

基础设施维护服务级别

① 一级：系统宕机，业务停止。

处理方式：即时响应，工作时间 30 分钟内，非工作时间 1 个小时内赶到现场，30 分钟内解决故障或给出经客户认可的故障解决方案。硬件设备出现故障时，应进行紧急备件更换，保证采购人业务的正常运行。

② 二级：系统能够工作，但部分功能失效。性能下降，但不至中断业务。

处理方式：即时响应，工作时间 30 分钟内，非工作时间 1.5 个小时内赶到现场，1 小时内解决故障或给出经客户认可的故障解决方案。

③ 三级：系统可以运行，但出现系统报错或出现问题。

处理方式：即时响应，工作时间 30 分钟内，非工作时间 2 个小时内赶到现场，2 小时内解决故障或给出经客户认可的故障解决方案。

3、技术团队要求

(1) 项目管理机构要求

运维服务要求 1 名非驻场项目经理，不少于 1 名驻场维护工程师，以及不少于 1 名 7×24 小时二线支持人员；采用人工、工具、现场和远程等多层面进行系统的监控及故障处理服务。

运维执行团队分为驻现场服务组 and 二线支持组，具体人员组成如下：

岗位	数量	主要职责	备注
项目经理	1 名	1. 负责管理整个维护服务项目； 2. 制订运维总体计划； 3. 对运维服务的质量、资源、风险等进行管理； 4. 设备运维管理，网络安全维护； 5. 软件系统、网络硬件巡检及维护管理。	非驻场
运维工程师	不少于 1 名	1. 执行具体的信息系统和网络硬件运维服务及运维管理； 2. 提交客户服务文档。	驻场
二线技术支持工程师	不少于 1 人	1. 负责月度巡检服务； 2. 负责二线技术支持； 3. 负责应急服务； 4. 协助完成项目的整体运维。	非驻场

(2) 技术能力要求

a. 项目经理

具有项目管理经验。按照项目管理的要求管理整个维护服务项目。对维护工作进行紧密跟踪和管理，协调与用户方之间的重大问题，对项目经理的职责应该在项目管理相关部分做充分的规定。

一般情况下，常驻人员的工作由项目经理安排和管理，对用户指定的管理员负责，同时用户指定的管理员可以安排和监督所有维护方人员的工作，如有必要用户方完全有权力调整维护人员的职责分工以及安排工作。

b. 驻场运维工程师

具有网络与信息安全从业经验。驻场运维工程师熟悉医院目前使用数据库及现有系统架构，参与过用户医院信息管理系统建设或维护服务经验，能够快速响应需求分析要求，提供解决方案。具备良好的表达和沟通能力，能够对用户进行相关维护培训，解决常见的维护问题。驻场人员接受采购人管理及工作调配，配合采购人对维保范围内各系统进行日常巡检维护，监控系统性能及稳定性，进行系统运行风险评估等。

c. 其他要求

医院现场驻守服务开始阶段必须有资深工程师和项目经理进行技术指导和培训工作。驻场工程师必须到位，未经用户方书面同意，不得更换驻场工程师；如果驻场工程师存在工作态度、责任心、技术能力、协调能力等方面之一的问题时，采购人有权要求维护方更换驻场工程师，并且维护方在收到采购人书面通知之日起 7 个工作日内必须更换，接替人员也必须经过面试、审核同意后才能开始试用，如果有两次以上的试用不合适，要求维护方进行整改，以公司名义正式提交整改报告。

4、保密要求

(1) 运维服务人员应严格遵守有关法规和政府内部规章制度，不得擅自翻阅、复制、传播所接触的用户资料或数据。

(2) 若需要更换设备，原设备必须先进行数据清洗，删除敏感数据并经用户检验后再回收。

(3) 在进行机房级网络安全运维过程中，将严格遵循保密原则，评估过程中将采取严格的管理措施，确保所涉及到的任何用户保密信息，不会泄露给第三方单位或个人，不得利用这些信息损害采购人利益。

(3) 安全检查和漏洞扫描的原始数据均存放在采购人提供的专用机器上，其它服务过程中相关的资料均应妥善保管，仅限在项目组内为本服务项目所用，不得以任何方式外泄或用于其它用途，服务人员应及时删除存储在电脑中或纸质的数据和文件材料。

5、维护登记制度

(1) 订立规范的维护流程和完善的文档，包括服务单和维护日志。在每次维护服务后详细记录维护单位、故障现象、维护内容、维护日期、维护结果、满意度等资料。

(2) 按季度和年度向提供电子版的维护报告和维护日志，为更好地开展维护服务工作提供依据。

(3) 对于重大维护事项，在实施前必须以书面形式向用户单位提供维护方案，经双方讨论确认。

6、项目风险管理

运维过程中须充分认识到项目风险管理的重要性，对风险进行分析，并提出相应的对策，应遵循以下原则：

(1) 规范性原则

根据项目管理方法，在人员、质量和时间进度等方面进行严格管控。

（2）标准化原则

严格遵守国家和行业的相关法规、标准，并参考国际的标准来实施。

（3）完整性原则

运维工作要综合考虑所维护设备的的技术和管理措施；作为一个完整有效的运维服务，应该是科学严谨的。任何疏忽或遗漏，都可能影响整个服务的结果。

7、项目培训要求

根据实际需求对用户进行系统培训，帮助用户熟悉软件的各项功能。

（1）培训目的：对用户进行全面的技术培训，使用户达到能独立进行管理、维护和故障处理等工作，以便保障软件产品能够正常、安全地运行。

（2）培训对象及资料：系统管理员和系统使用人员。必须要提供培训教材。所有的培训资料必须是中文书写。

8、文档交付要求

应用系统和网络硬件运维应严格按照国家软件工程规范等标准进行，根据维护服务工作的开展按要求提供有关文档。