江苏省政府采购合同（服务）

项目名称：信息相关设备运维及安全服务

项目编号：JSZC-320200-SXZT-G2025-0044

甲方：无锡市第二人民医院

乙方：江苏中铭慧业科技有限公司

甲、乙双方根据无锡市公共资源交易中心信息相关设备运维及安全服务项目公开招标的结果，签署本合同。

一、合同内容

1.1 标的名称：信息相关设备运维及安全服务

1.2 标的质量：见附件 3：服务考核

1.3 标的数量（规模）：见附件 1：运维项目清单和设施清单

1.4 履行时间（期限）：2025 年 12 月 1 日-2026 年 11 月 30 日

1.5 履行地点：无锡市第二人民医院

1.6 履行方式：见附件 2：运维技术和服务要求

二、合同金额

2.1 本合同金额为（大写）：柒拾柒万元整（770000 元）人民币，含税。

三、技术资料

3.1 乙方应按招标文件规定的时间向甲方提供服务（包含与服务相关的货物）的有关技术资料。

3.2 没有甲方事先书面同意，乙方不得将由甲方提供的有关合同或任何合同条文、规格、计划、图纸、样品或资料提供给与履行本合同无关的任何其他人。即使向履行本合同有关的人员提供，也应注意保密并限于履行合同的必需范围。

四、知识产权

4.1 乙方应保证甲方在使用、接受本合同服务（包含与服务相关的货物）或其任何一部分时不受第三方提出侵犯其专利权、版权、商标权和工业设计权等知识产权的起诉。一旦出现侵权，由乙方负全部责任。

（注：采购项目如涉及采购标的的知识产权归属、处理的，如订购、设计、定制开发的信息化建设项目等，应当约定知识产权的归属和处理方式）

五、产权担保

5.1 乙方保证所交付的服务（包含与服务相关的货物）的所有权完全属于乙方且无任何抵押、查封等产权瑕疵。

六、履约保证金

6.1 乙方交纳人民币\元作为本合同的履约保证金。（不得超过合同金额的 10%）

6.2 合同履行结束后，甲方应及时退还交纳的履约保证金。

6.2.1 履约保证金退还方式：\

6.2.2 履约保证金退还时间：\

6.2.3 履约保证金退还条件：\

6.2.4 履约保证金不予退还的情形：\

七、合同转包或分包

7.1 乙方不得将合同标的转包给他人履行。

7.2 乙方应按招标文件要求，如项目不允许分包的，乙方不得将合同标的分包给他人履行；如项目允许分包的，乙方应当按照投标文件中提供的分包意向协议履行合同。

7.3 乙方如有转包或未经甲方同意的分包行为，甲方有权解除合同。

八、合同款项支付

8.1 合同款项的支付方式及进度安排

8.1.1 预付款支付时间：合同签订生效后支付，预付款支付比例：合同金额的 50 %，计人民币叁拾捌万伍仟元整（385000 元）。

8.1.2 尾款支付时间：服务结束并验收合格后支付,尾款支付比例：合同金额的 50 %，计人民币叁拾捌万伍仟元整（385000 元）。

8.2 付款方式：乙方在付款前向甲方提供等额的合规服务发票；乙方逾期交付符合要求的发票和材料，甲方有权延迟付款；乙方未能按照合同约定的内容提供相应服务，甲方有权减少或拒绝支付服务费；如甲方因故无需乙方提供本合同约定的完整服务期限，可根据乙方实际服务期限按实结算。

8.3 双方银行信息

8.3.1 甲方的开票信息：

户名：无锡市第二人民医院

纳税人识别号：123202004662860049

开户银行：江苏银行无锡新生路支行

账号:870010188900003838

发票接收人:陈宇昂 15961836805

8.3.2 乙方开户银行：

开户银行：中国银行钱桥支行

地址：无锡市南湖大道 855 号扬名科创中心 19 层

帐号：523558200704

九、税费

9.1 本合同执行中相关的一切税费均由乙方负担。

十、项目验收

10.1 甲方依法组织履约验收工作。

10.2 甲方在组织履约验收前，将根据项目特点制定验收方案，明确履约验收的时间、方式、程序等内容，并可根据项目特点对服务期内的服务实施情况进行分期考核，综合考核情况和服务效果进行验收。乙方应根据验收方案内容做好相应配合工作。

10.3 对于实际使用人和甲方分离的项目，甲方邀请实际使用人参与验收。

10.4 如有必要，甲方邀请参加本项目的其他供应商或第三方专业机构及专家参与验收，相关意见将作为验收书的参考资料。

10.5 甲方成立验收小组，按照采购合同的约定对乙方的履约情况进行验收。验收时，甲方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，出具验收书，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存档备查。

10.6 验收合格的项目，甲方根据采购合同的约定及时向乙方支付合同款项、退还履约保证金。验收不合格的项目，甲方依法及时处理。采购合同的履行、违约责任和解决争议的方式等适用《中华人民共和国民法典》。乙方在履约过程中有政府采购法律法规规定的违法违规情形的，甲方将及时报告本级财政部门。

十一、违约责任

11.1 甲方无正当理由拒绝接受乙方提供服务的，甲方向乙方偿付拒绝接受服务合同价款总值____的违约金。

11.2 甲方无故逾期验收和办理合同款项支付手续的，甲方应按逾期付款总额____每日向乙方支付违约金。

11.3 乙方逾期提供服务的，乙方应按逾期提供服务合同总额每日千分之六向甲方支付违约金，由甲方从待付合同款项中扣除。逾期超过约定日期 10 个工

作日不能提供服务的，甲方可解除本合同。乙方因逾期提供服务或因其他违约行为导致甲方解除合同的，乙方应向甲方支付合同价款总额 20% 的违约金，如造成甲方损失超过违约金的，超出部分由乙方继续承担赔偿责任。

11.4 乙方所提供服务的标准不符合合同规定及招标文件规定标准的，甲方有权拒绝接受服务，并可单方面解除合同。

十二、不可抗力事件处理

12.1 在合同有效期内，任何一方因不可抗力事件导致不能履行合同，则合同履行期可延长，其延长期与不可抗力影响 期相同。

12.2 不可抗力事件发生后，应立即通知对方，并寄送有关权威机构出具的证明。

12.3 不可抗力事件延续 120 天以上，双方应通过友好协商，确定是否继续履行合同。

十三、解决争议的方法

13.1 双方在签订、履行合同中所发生的一切争议，应通过友好协商解决。如协商不成，由甲方住所地人民法院管辖。

十四、合同生效及其它

14.1 合同经双方法定代表人或授权委托代表人签字并加盖单位公章后生效。

14.2 本合同未尽事宜，遵照《中华人民共和国民法典》、《中华人民共和国政府采购法》有关条文执行。

14.3 本合同正本一式肆份，具有同等法律效力，甲方执叁份，乙方执壹份。

甲方：无锡市第二人民医院

地址：无锡市中山路 68 号

2025年12月11日

法定代表人或授权代表：

联系电话：0510-68562222

乙方：江苏中铭慧业科技有限公司

地址：无锡市梁溪区南湖大道 855 号 1901 室

法定代表人或授权代表：

联系电话：0510-85750746

签订日期：2025 年 12 月 11 日

附件 1：运维项目清单和设施清单

表 1 运维项目清单

序号	项目名称	项目及运维内容介绍	分项价格（万元）
1	物联网冷链管理系统	为医院日常运营中涉及包括药品、试剂、血液产生、运输、仓储、使用等提供支撑。明细详见运维设施清单。	4.7
2	HIS 数据库及核心设备	医院现有的 HIS 数据库承载着大量的患者信息，且每天会新增大量的数据，需要对该数据库及相关设备进行专业的运维服务和技术支持，同时提供配件的免费维修和更换服务。明细详见运维设施清单。	13.2
3	弱电运维	医院有大量的办公终端、门禁设备、PDA 设备和网络系统，需要专业服务保障设备的正常运行。明细详见运维设施清单。	19.62
4	互联网门户网站	医院互联网网站需要相关维护服务保证其正常运行，需及时修改和维护网站内相关内容，同时要对网站的互联网域名做好域名续费、域名解析、指向及企业电子信箱链接等服务。	0.78
5	信息机房 UPS 和精密空调	对两个院区的所有信息机房内 UPS 和精密空调等设施设备进行维护保养，目前共包括五套 UPS 系统及电池，六套精密空调及其相关配套基础设施。其中 UPS 主机及电池需要定期进行检测，空调除故障维修外，也需要定期进行清洁，以确保设备的持续工作。明细详见运维设施清单。	7.47
6	无线网络	医院无线内网，主要承载医疗应用类终端设备的使用，主要运维无线网络相关的设备及配件，提供硬件产品的免费维修服务，并定期及按需提供网络检测服务。明细详见运维设施清单。	5
7	LED 大屏运维	目前医院两个院区总计有彩屏三块，单色屏十八块。这些大屏主要分布在各大楼室内外人员比较密集的地方，用于发布医院的动态信息、排队窗口的抬头显示，需要提供专业的运维服务和技术支持。	3.93
8	网站安全云防御	为 Web 系统提供 100%的安全防御支持，实现对中心互联网网站安全防护；同时面向统一防护能纵向查看网站所有访问历史数据，对攻击进行溯源，弥补传统 WAF 单纯依靠规则的局限性，保障 Web 系统安全运行。	2.3
9	安全服务	医院目前有各类安全设备 30 余套，这些设备在出口边界、安全计算、安全管理等区域存在极大的作用，为合理发挥安全设备更大的作用，需要有安全运营能力的单位将这些安全硬件、系统等有机融合，发挥更大的效用，从而全面提升医院的信息化安全运营能力。明细详见运维设施清单。	20

表 2 运维设施清单

序号	名称	型号规格	说明	数量
1	无线网络设备（南院 1 号楼）	WIDS-1000-22 plus	增强型 WLAN 室内分布系统基站	9
2		WIDS-1000-12 plus	增强型 WLAN 室内分布系统基站	2
3		WIDS-1000-10 plus	增强型 WLAN 室内分布系统基站	4
4		OF-S2402	WIDS 功分器	99
5		OF-C240X	WIDS 耦合器	148
6		OT-24XZ03D	WIDS 医疗专用天线	262
7		RF1/2″ BHF	1/2″馈线	2500
8		AC2010	昂科无线宽带接入控制系统	1
9		WIDS-HD-5110	11AC 基站	2
10		OT-0460VS	400M-6G 超宽频医疗专用天线	133
11		OF-S046002S	400M-6G 超宽频二功分器	46
12		OF-S046003S	400M-6G 超宽频三功分器	21
13		OF-C04600XS	400M-6G 超宽频耦合器	45
14		RF50Z 1/2″	1/2″阻燃线缆	1350
15		1/2″N-X	射频连接器（X：J/K/JJ）	509
16	生产库小型机	IBM Power 750	最新 AIX 操作系统，HACMP 集群软件，含 HMC 控制台	2
17	光纤交换机	DELL Brocade 300	8Gb 光纤交换机，配置 7 个 8Gb 多膜短波，含 8 对光纤跳线	2
18	历史库小型机	IBM Power 570	最新 AIX 操作系统，HACMP 集群软件，含 HMC 控制台	2
19	备份测试小型机	IBM Power 570	最新 AIX 操作系统，HACMP 集群软件，含 HMC 控制台	1
20	HIS 数据库	ORACLE	HIS 核心库、包含历史库及查询库等。	1
21	UPS	APC SY48K48H-PD(48KVA)	南院 1 号楼中心机房	1
22		艾默生 160KVA	南院 1 号楼地下二层 UPS 机房	1
23		APC SY12K16H（12KVA）	南院容灾机房	2
24		山特 3C3-40KS(40KVA)	南院门诊负一楼机房	1
25		山特 3C10KS(10KVA)	南院行政楼电工房弱电间	1
26	精密空调	艾默生 PEXP2040FA(40KW)	南院 1 号楼中心机房	2
27		克莱门特 SAF013/1*C17(13KW)	南院 1 号楼地下二层 UPS 机房	1
28		克莱门特	南院容灾机房	1

		SAF020/1*C24(20KW)		
29		RC 43.6KW	北院行政楼 8 楼中心机房	2
30		RC 21KW	北院行政楼 8 楼中心机房	1
31		DME 12.5KW	北院行政楼 A 楼 B 层机房	1
32	动力环境监控	APC	南院 1 号楼中心机房	1
33	KVM 系统	APC	南院 1 号楼中心机房	1
34	配电系统		南院 1 号楼中心机房	1
35	LED 大屏	南院彩屏	定期检查，软件升级，性能监控，备品备件，紧急响应等	1
36		南院单色屏		6
37		北院彩屏		2
38		北院单色屏		12
39	超低温标签	SYRIS SYTAG245-HT1-2YD	双向冷链标签，超低温度检测，温度范围：-40℃~-86℃/±0.4℃ RFID 传输	3
40	低温标签	SYRIS SYTAG245-HT-V2.0	双向冷链标签，温湿度检测，防泼水外壳,LED 显示,2.45 GHz 支持双向通讯	120
41	物联网接收器	SYRIS SYRD245-1N-V2.0	2.4GHz 支持双向通讯，防碰撞机制，可同时读取多数标签，2 组继电器输出点	25
42	冷链管理系统	定制	全院 15 个科室物联网冷链监视	1
43	办公设备	戴尔/联想/惠普/宏基/神舟等	包括计算机及外设软硬件故障维修、系统安装调试、设备迁移等	3000
44	网络系统	/	信息点调整及网络终端故障的处理	按需
45	门禁	金凯/中控/大华等	包括系统故障检测及故障设备的维修	按需
46	可视门铃	金凯/天图/星光楼宇等	包括系统故障检测及故障设备的维修	按需
47	PDA 终端设备	BayNexus/东集/盈达	PDA 终端设备维护，备品备件及维修	450
48	互联网门户网站	/	含域名续费、域名解析等服务	1
49	网站	/	防护服务，服务周期内防护引	1

	安全云防御		擎、防护规则免费升级。包含 Web 攻击防护服务；DDoS 攻击共享型防护服务；CC 攻击防护服务；网站缓存加速；非标端口配置；5TB/年免费流量。	
50	安全服务	风险评估服务	每年一次	1
51		渗透测试服务	每年二次	2
52		应急响应服务	每年二次	2
53		安全分析服务	每年二次	2
54		安全加固服务	每年二次	2
55		安全培训服务	每年一次	1
56		基础架构梳理	每年一次	1

附件 2：运维技术和服务要求

一、技术要求：

（1）保障运维设施及相关系统能正常运行，出现故障能及时解决；同时配合甲方的管理需求配合服务。

（2）如相关项目或系统接收到上级部门安全通报，或甲方安全扫描发现相关网络安全问题，应在指定期限内无条件完成安全修复。

（3）数据中心整体集成服务要求：

①数据库性能调优，根据应用系统实际情况，对数据库进行调优，保证应用稳定运行。

②提供 HIS 数据库存储双活维护工作。

③对现有系统中核心业务表按照年度时间等条件进行优化处理，确保生产库的使用效率。

④对数据库进行定期巡检，并实时优化 SQL 语句。

⑤数据库软件升级，根据应用系统要求或者实际情况，对数据库版本进行更新补丁。

⑥不定期对系统运行部署进行适当优化调整，以满足快速恢复系统运行要求（需经甲方同意）。

⑦要特别关注单点故障维保工作。单点故障是指该故障点出现问题将会使该点涉及的系统瘫痪，因此要做好单点故障点的排查以及应急方案，日常做好系统备份工作，并将必要的备品备件安放在甲方现场，以备系统瘫痪时可以及时更换，确保系统在最短的时间内恢复正常。

⑧主动及时记载数据中心各方面的运行数据，并根据实际情况协调各厂商进行系统性能调整以满足运行要求。

⑨适时做好预防性维护，发现系统隐患及时解决，重视甲方的提醒和建议。

⑩配合软件厂商进行系统规划、调优、修复，根据数据中心的运行情况提前提出设备更新、扩容、升级建议。

⑪提供专业工程师现场服务，每周至少 1 个工作日在现场实时监控数据中心运行情况，解决疑难问题，并按时提供数据中心运行月报。

⑫由于目前 HIS 数据库的数据量已经超过 1.8T，数据库压力增加，因此乙方在保障业务的同时需无缝将常用的生产数据库和历史数据进行库分离操作，利用现有设备（历史库服务器）搭建历史库，从而保证生产库中保留近三年数据，并提供历史库给业务查询，同时提供简便易用的可视化的数据归档操作界面。

⑬利用备份测试服务器，建设逻辑第三数据库服务和数据库备份服务，满足逻辑错误的恢复。

⑭提供系统健康检查、故障应急预案和系统调优规划，并提交相应的健康检查报告。

⑮建立系统运行维护档案，提供调优建议方案。

⑯为预防由于安全漏洞带来的系统宕机、数据丢失等风险，需提供系统备份、恢复等方面的服务。

⑰按照甲方要求提供相应的小型机技术服务，如中标单位无能力处理时需要在规定时间内提供必要手段保证系统的稳定运行。

⑱提供相应的现场技术支持及 HACMP 技术支持服务（包括安装、管理和维护），同时提供必要的其他相关业务系统数据库的技术支持服务。

⑲提供定期巡检服务，至少每月 1 次。

（4）LED 大屏服务要求：

①维护范围：LED 显示屏系统包括其相关联的所有软件系统（LED 显示屏音视频控制系统）和硬件设备（其中硬件部分含 LED 显示屏显示单元模组、发送系统、接收系统、视频处理器、视频拼接器、控制电脑、开关电源、电源控制柜、信号连接线缆、电源连接线缆、显示屏钢结构等相关设备）提供保质期外的技术支持、检修、维护、升级、保养服务。

②提供原厂零配件，不因配件缺失、设备老旧等原因拒绝后续维修服务。

（5）网站安全云防御服务要求：

①Web 攻击防护服务，需包含：跨站攻击、伪造请求攻击、SQL 注入、上传漏洞攻击、后门植入等 WEB 漏洞攻击防护。

②DDoS 攻击共享型防护服务，最高不超过 8Gbps 的防护，需包含常见的 DDoS 攻击类型的防护。

③CC 攻击防护服务（CC 攻击频率 2 万 Q/S）：防护基于应用层的 DDoS 攻击防护。

④网站缓存加速，需包含对静态资源缓存，降低源站负载，提升访问速度。

⑤非标端口配置，至少需包含 5 个，21、22、80、443、445、3389 等端口可除外。

⑥每月为所防御的门户网站出具安全云防御报告。

（6）安全服务要求：

①风险评估服务：对甲方信息资产面临的威胁、存在的脆弱性、现有防护措施及综合作用而带来风险的发生可能性进行评估，最终提供完整的风险评估报告及修复建议，提交《风险评估报告》，服务周期内至少一次。

②渗透测试服务：需以主流渗透工具发现互联网上行业发布的系统，以常见的高中危漏洞为主要目标，将发现的安全漏洞进行整理，给出详细说明，针对安全漏洞逐一提供相应的解决方法。并结合修复情况，协助针对修复后的漏洞进行复测验证，最终提交《业务系统渗透测试报告》，在服务周期内每半年进行一次。

③应急响应服务：当发生外部黑客入侵、数据泄露、木马病毒等突发安全事件时，提供包括事件检测与分析、风险抑制、问题处置、协助业务恢复的服务，协助甲方快速止损，最大化降低安全事件带来的影响，并在应急响应协助后及时提交《应急响应报告》，服务周期内至少提供两次。

④安全分析响应服务：运用丰富的技术经验及威胁情报知识库，借助态势感知平台设备对接能力及安全检测能力对安全日志、流量进行分析研判并对发现的威胁进行定位，同时提供对态势感知平台告警、日志、报告等信息的解读，提供《安全分析报告》，服务周期内每半年进行一次。

⑤安全加固服务：根据评估和测评等检测的结果及整改意见，对 WEB 应用、网络设备、操作系统、数据库等不涉及业务的安全配置进行加固。定期配合其他服务商对安全系统和对应软件产品进行迭代升级；依赖特征库的，定期进行特征库升级；根据安全威胁情报、评估测评检测结果、业务需求等，通过一系列技术和流程来加强信息系统、网络和应用程序的安全性，以防范潜在的安全威胁和攻击。此项服务旨在通过甲方已发现的潜在漏洞和弱点，采取相应的措施来加强系统的防御能力。针对各类网络及网络安全资产、各类服务器和存储设备，依据漏扫、测评结果等进行升级加固、策略优化，以达到安全加固的目标，针对变更提交《配置变更报告》、针对升级加固提交《安全加固报告》，服务周期内不少于两次。

⑥安全培训服务：根据甲方需求，邀请信息安全专家，组织信息安全专题培训，全面提升甲方信息安全从业人员对常见网络安全问题的洞察能力，熟悉网络安全问题的解决和处理方法，进一步提升专业技术水平，同时了解国家相关法律法规政策。服务周期内至少提供一次。

⑦基础架构梳理：根据国家政策法律法规及甲方需求，结合医疗行业属性，按需调整安全部署。通过一系列安全措施、技术和流程，确保甲方信息系统的机密性、完整性和可用性。根据安全架构的梳理，提升信息系统的安全性和稳定性，要求架构梳理过程不影响甲方正常业务开展，在服务周期内至少提供一次。

（7）保驾护航服务：在重要活动或任务需要技术保障时，需按甲方要求派遣技术人员在现场提供保驾护航服务。

（8）其他要求：

①提供在正常条件下保证运维项目中系统正常稳定运行的系统扩充、版本更新升级及功能更新服务；提供在正常条件下改进系统性能的各项建议，包括系统资源分配与效率改进建议，软件配置规划和性能优化建议，系统容量预测建议等。

②当项目内设施外部环境或数据环境发生变化，须按要求无条件配合修改、迁移（包括系统及数据的备份、恢复、迁移等）以适应变化。

③根据甲方需求免费提供相关报表、数据查询统计等数据服务。

④因系统需要、政策性要求等情况，需调整或新增视图做对接或上报的，须按要求无条件执行，不得以任何理由拒绝或拖延。

⑤提供运维服务期间需最大程度减少对在线系统的影响，不可随意实施导致在线系统停止服务，否则甲方有权终止合作并向服务商追偿。另外，如因运维的设备或系统故障处置不力，从而导致甲方直接经济损失的，应向甲方赔偿相应金额损失（因甲方原因造成故障除外）。

二、服务要求：

①项目服务期：一年（2025 年 12 月 1 日-2026 年 11 月 30 日）。

②日常巡检：每季度至少 1 次巡查各项目（有特殊巡检要求的以相关条款要求为准），按照维保巡检管理规程的相关要求，对软硬件设备运行状态、运行环境等进行检查与评估，每次巡检应提供巡检报告，并根据巡检报告，及时与用户进行交流，及时协调解决工作中的问题。如甲方需要在指定日期进行单项巡查相关系统，须按要求无条件执行。

③服务响应及修复时间：需提供 1 年 7*24 小时热线服务响应和支持，同时维护服务工作需要综合采用多种方式来完成具体工作内容，以满足维护工作对时效的高要求，具体包含实时远程运维派单，出现故障节点时能及时发现并通过安全专线进行远程第一时间处理，并提供多途径远程支持服务、夜间及节假日轮换值备班、接到通知后 15 分钟内的紧急现场服务等几种方式；一般类故障应在 2 小时内进行修复，特殊复杂类故障双方可协商修复时间（但需确保医院的正常业务开展），但预估超过 8 小时的故障必须提供应急方案或备件确保系统运行。修复后 7 日内回访一次，确保修复后系统的正常工作状态。

④现场技术服务：要求弱电运维提供一位资深 5*8 现场技术服务工程师，配合甲方的日常网络设备、终端设备、门禁设备等的运维工作和各项临时性指派任务，负责日常维护、收集需求、现场解决问题等；现场技术服务工程师须遵从甲方的工作时间和工作地点的安排，接受甲方的服务考核。投标单位提供的现场技术服务工程师必须具备应有的技术能力和经验且经甲方确认后方可上岗。甲方如对中标单位提供的人员不满意，经声明后，中标单位须及时更换人员，直至甲方

满意为止。现场技术服务工程师需对甲方情况有良好的了解，并应当保持服务人员相对稳定，非特殊原因不得随意更换；如确有需要更换的，中标单位应安排有相关工作经验的人员，并提前一个月到现场进行工作交接获得甲方同意后，方可更换。

⑤项目交付物：提供完整服务期限的维保服务，在运维服务结束时进行运维验收并交付各阶段和年度的运维服务报告，包括但不限于验收报告、季度巡检报告、运维服务阶段性小结、运维服务年度总结、运维服务记录单等。

⑥咨询服务：对医院信息系统进行定期的维护管理和配置优化，确保医院整个信息系统运转的高效、稳定和安全，减少和避免系统性能瓶颈，杜绝信息系统安全事故，并且能根据用户需要，提供信息系统运行的合理化建议和方案。针对系统常规运行要求，提出符合实际要求的升级建议。

⑦除上述所述通用性服务要求以外，个别系统还需提供以下要求服务：

a. 物联网冷链管理系统需定期对冷链电池提供监测和更换服务（电池由甲方自行采购），以确保其正常运行，至少每月一次。

b. 互联网门户网站需主动进行网络备份和页面修改等服务，按需可根据甲方实际拥有的最新备份数据，进行数据恢复；对网站服务器、服务器防护软件、企业域名防护证书、后台管理系统等进行扩容和安全升级。

c. 信息机房 UPS 需定期检查电池状态，以确保电池的稳定运行状态，年均 2 次。信息机房精密空调需定期清洁和保养，包括过滤器更换和内部清洁，以确保良好的空气质量和冷却效率，年均 4 次。评估 UPS 和精密空调的能效，提供优化建议，以减少能源消耗和运营成本，年均 1 次。

d. 定期检查全院 LED 大屏，包括对 LED 模块、电源、控制系统、通信设备等的检查和保养，以确保其正常运行，至少每月一次。并定期对大屏控制系统和软件提供升级服务，以确保其与最新技术和功能兼容，同时修复已知的漏洞和问题。

附件 3：服务考核

表 3 服务质量考核表

运维分项：

考核类别	权重	考核子类	考核指标	考核要求	分值	考核结果
服务团队	20%	工作纪律	服务人员的工作纪律情况，有无违反现场规定的行为。	根据问题的严重性分为三档 1）一般，扣 1 分； 2）较严重，扣 2 分； 3）十分严重，扣 5 分	5	
		技术能力	服务人员的技能、沟通和管理各项能力是否满足现场需求。	根据问题的严重性分为三档 1）一般，扣 1 分； 2）较严重，扣 2 分； 3）十分严重，扣 5 分	5	
		工作态度	服务人员责任心，服务态度，开展相关工作的积极性。	根据问题的严重性分为三档 1）一般，扣 1 分； 2）较严重，扣 2 分； 3）十分严重，扣 5 分	5	
		规范性	服务团队的维护规范性，有无因规范性引发不必要的故障问题。	根据问题的严重性分为三档 1）一般，扣 1 分； 2）较严重，扣 2 分； 3）十分严重，扣 5 分	5	
服务实施	70%	服务内容完整性	服务内容是否按照服务要求和目标严格执行。	服务内容缺失 1 项扣 5 分，本条目扣完为止。	15	
		响应及时性	是否及时响应并处置故障报修。报修响应状态和结果是否及时回复。	出现响应不及时或“未处置”事件，出现一次则不合格扣 5 分，本条目扣完为止。	15	
		安全性	服务过程中是否出现安全事故或处置不当导致业务中断等不利情况。	出现安全事故本条目分值扣完； 出现因服务导致业务中断等不利情况扣 5 分，本条目扣完为止。	40	
服务管理过程	10%	文档完整性	服务相关报告是否按时提交，且质量符合要求。	出现一次不及时扣 2 分，质量不满足要求扣 2 分，本条目扣完为止。	10	
合计					**100**	

年度考核结果直接与服务合同付款金额挂钩，考核采取百分制，划分为 A、B、C、D 四个等级，以考核评定为准。各个等级对应分数及支付比例情况如下：

表 4 等级对应表

等级	运维分项考核分数（N）	支付金额
A	90≤N≤100	100%
B	70≤N＜90	85%
C	60≤N＜70	60%
D	N＜60	运维费尾款中的分项金额不予支付，同时采购人有权终止该服务合同中的分项内容并要求服务商退还采购人已支付的分项金额