2025 年度长宁区卫生数据中心硬件维护服务项目

需求文件

第 1 章　项目概述

1.1　项目背景和概述

自 2006 年长宁区开展卫生信息化建设至今，已经建设了覆盖全区的医疗卫生机构的卫生健康信息网，有机地整合公共卫生、基本医疗、卫生经济等系统，实现多种信息模式的协同，通过区域数据中心管理交互门户和居民健康在线咨询门户，实现医院、卫生机构、社区卫生服务中心、居民家庭卫生健康信息的互联互通。

长宁区域卫生信息平台建设初期进行了统一规划，硬件设备均提供了独立的数据库服务器、应用服务器，并具有相关的备份容灾手段，如双机热备，异地备份等。通过前期基础数据中心以及区域卫生信息平台两期对基础设施的升级改造，上海市长宁区公立医院和社区卫生管理中心已经建立了满足市级区域卫生信息平台（含市卫生数据中心）运行包括服务主机、数据交换、存储、备份和安全设备等组成的基础设施环境。

随着长宁区医疗卫生信息化的发展，区卫生数据中心项目不断发展和完善，目前长宁区卫生健康委员会卫生信息数据中心的硬件产品、系统软件、安全产品和数据中心应用系统运行平稳，且已经进入有偿服务期，为保障各信息系统安全、连续、可靠的有效运行，本次项目拟对 2025 年长宁区卫生数据中心硬件维护服务进行采购。

由响应人为长宁区卫生健康委员会卫生信息数据中心的硬件产品、安全产品和机房环境监控系统提供运行维护保修服务工作，发挥专业运维优势，保障各信息系统的安全、连续、可靠的有效运行。

本次采购内容为对长宁区卫生数据中心的硬件产品、安全产品和机房环境监控系统购买运行维护保修服务。本次采购范围为一年的维保服务。

1.2 服务目标

本项目由专业运维服务商承担数据中心系统软硬件设备的运行维护工作，提供系统软硬件设备保修维护及技术支持服务，处理相关系统技术问题，紧急故障响应，为长宁卫健委核心系统设备提供维护保障，从而确保长宁卫健委业务系统的安全、连续、可靠、有效运行。

1.3 服务地点

长宁区卫生数据中心。

1.4 服务内容

序号	分类	维护内容	服务方式和内容	授权	续保年限
1.	硬件产品	网络设备保修与服务	维保服务、备品备件库服务	否	一年
		服务器设备保修与服务	维保服务、备品备件库服务	否	一年
		存储设备保修与服务	维保服务、备品备件库服务	否	一年
		安全设备保修与服务	维保服务、备品备件库服务	是	一年
2.	机房环境监控	机房环境监控运维	故障响应、定期日志维护	否	一年

1.4.1 服务器情况

长宁区卫生数据中心信息平台服务器根据使用情况主要包括以下 5 大类型：

1. 区域卫生平台数据库服务器：独立数据库服务器，置于长宁区卫健委中心机房。

2. 区域卫生平台应用虚拟机：支撑区域平台应用、区域健康档案应用、区域家庭医生应用等，置于长宁区卫健委中心机房。

3. 备份服务器：备份服务器支持实时和定时的备份机制，置于长宁区卫健委中心机房。

4. 管理服务器：包括部署了安全软件的管理服务器，置于长宁区卫健委中心机房。

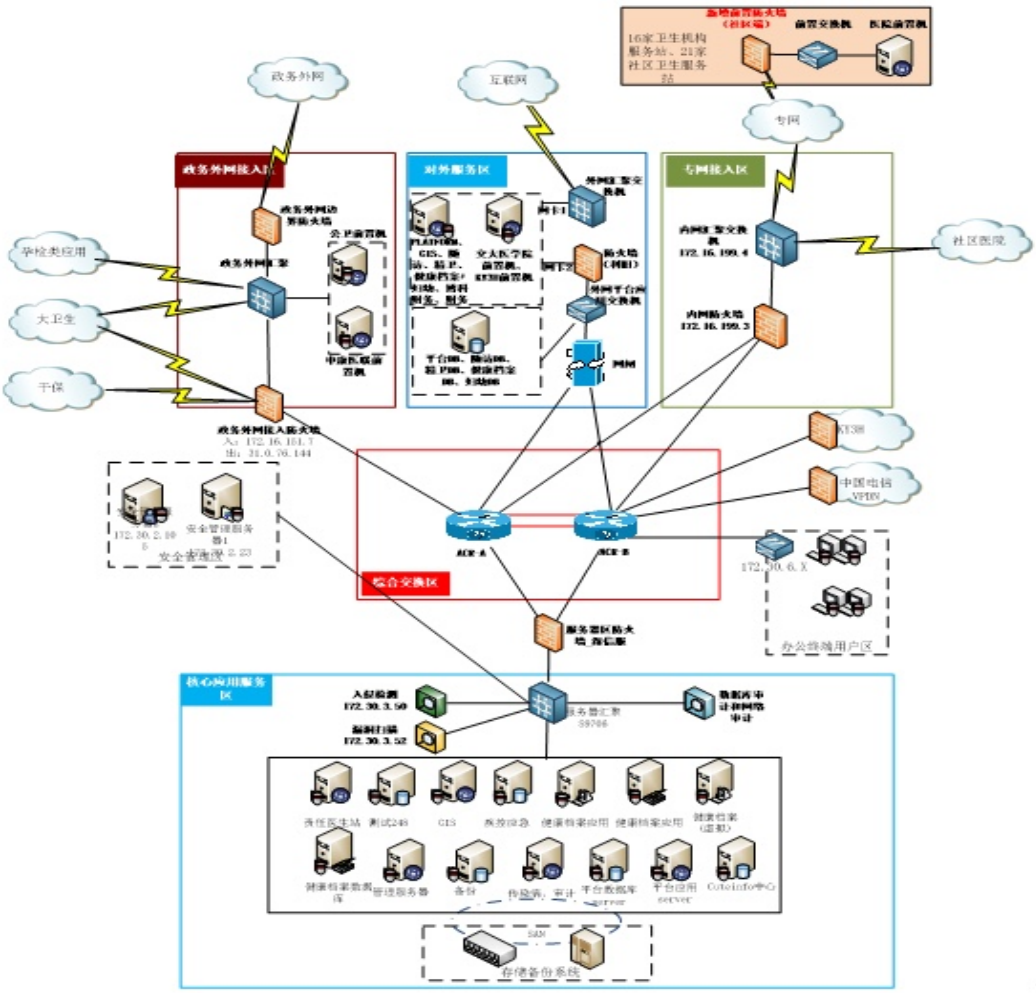
5. 前置机：作为二级医院或者社区卫生服务器中心前置机，置于各家医疗机构。

1.4.2 存储情况

长宁区卫生数据中心信息平台已建设有总容量达 18T 的 EMC 大容量在线存储设备及电信异地容灾备份。

1.4.3 网络设备情况

长宁区依托电子政务外网和卫生专网光纤，建立了上联市卫健委、市政府，横联区政务事业单位，下联区属卫生医疗机构的卫生系统虚拟专用网络。



长宁区域平台网络拓扑图

1.4.4 机房环境

机房环境监控系统对机房环境状况进行监控，监控内容包括：供电系统、ups系统、精密空调系统、机房温湿度、漏水检测等。

第 2 章　项目目标

2.1　服务周期

本项目服务期为：1 年。

2.2　运维服务总则

1. 安全性

由于长宁区卫生信息数据中心部署了长宁卫生健康委员会的核心业务系统，因此必须确保系统的设备安全、有效，并且在出现故障后能得到及时的修复，在出现损坏的情况下，应能及时进行备件更换。

2. 可用性

应尽可能保障长宁区卫生信息数据中心的设备的稳定运行，确保长宁卫生健康委员会的核心业务系统的可用性，尽可能减少故障的发生。

3. 保护原有投资

国家财政要求尽可能保护原有的投资，因此，将采用“有保续保”的原则，尽可能采用购买续保的方式，对原有系统的设备进行充分的利用，保护原有投资。

2.3　服务总体要求

1. 提供5×8常驻现场服务，每日检查系统运行情况，第一时间发现和解决故障。
2. 在突发事件发生时提供7×24小时的服务和驻点保障，并且配备相应的人员予以积极配合。
3. 如有驻场工程师临时离开，需向医管中心提前请假。
4. 保证应用系统灾难性恢复，保证一般灾难情况下系统发生不能运行时的2小时诊断、4小时基本修复的要求。
5. 保证系统不发生重大安全问题，保密数据没有外泄。网络和安全策略得

到有效保障。

6. 定期对系统进行性能监控，保持系统运行过程中性能稳定。

7. 完成对用户方的技术培训。

2.4 硬件产品维保部分

2.4.1 服务器存储及网络产品清单

序号	硬件名称	型号	数量	服务方式和内容	服务范围	服务级别
1	刀片服务器机箱	HP C7000	1	维保服务、备品备件库服务	区域卫生数据中心	7*24
2	刀片服务器	HP BL680C G5	3	维保服务、备品备件库服务	区域卫生数据中心	7*24
3	刀片服务器	HP BL480C G1	2	维保服务、备品备件库服务	区域卫生数据中心	7*24
4	刀片服务器	HP BL460C G1	15	维保服务、备品备件库服务	区域卫生数据中心	7*24
5	内网应用服务器	IBM X3650 M2	2	维保服务、备品备件库服务	区域卫生数据中心	7*24
6	外网数据库及应用服务器	IBM X3850 M2	2	维保服务、备品备件库服务	区域卫生数据中心	7*24
7	内网数据库服务器	IBM X3850 M2	2	维保服务、备品备件库服务	区域卫生数据中心	7*24
8	内网存储设备	存储 IBM DS3400	1	维保服务、备品备件库服务	区域卫生数据中心	7*24
9	外网存储设备	存储 IBM DS4700	1	维保服务、备品备件库服务	区域卫生数据中心	7*24
10	PC 服务器	DELL R710	14	维保服务、备品备件库服务	区属医疗机构	7*24

11	PC 服务器	联想 Think Server SR630	10	维保服务、备品备件库服务	区属医疗机构	7*24
12	PC 服务器	DELL R720	8	维保服务、备品备件库服务	区域卫生数据中心	7*24
13	光纤交换机	Brocade 300	2	维保服务、备品备件库服务	区域卫生数据中心	7*24
14	PC 服务器	联想 Think Server RD630	2	维保服务、备品备件库服务	区域卫生数据中心	7*24
15	PC 服务器	联想万全 R680	2	维保服务、备品备件库服务	区域卫生数据中心	7*24
16	存储	联想 EMC 存储 VNX 5300	1	维保服务、备品备件库服务	区域卫生数据中心	7*24
17	PC 服务器	联想 Think Server RD630	2	维保服务、备品备件库服务	区域卫生数据中心	7*24
18	PC 服务器	IBM X366	1	维保服务、备品备件库服务	区域卫生数据中心	7*24
19	PC 服务器	DELL R730	2	维保服务、备品备件库服务	区域卫生数据中心	7*24
20	PC 服务器	HP DL388 GEN10	4	维保服务、备品备件库服务	区域卫生数据中心	7*24
21	服务器	浪潮 SA5212M5	1	维保服务、备品备件库服务	区域卫生数据中心	7*24
22	存储	DELL SCv2020	1	维保服务、备品备件库服务	区域卫生数据中心	7*24
23	光纤交换机	CISCO 光纤交换机	2	维保服务、备品备件库服务	区域卫生数据中心	7*24
24	小型机	IBM Power 740	2	维保服务、备品备件库服务	区域卫生数据中心	7*24

25	存储	EMC VNX5500	1	维保服务、备品备件库服务	区域卫生数据中心	7*24
26	PC 服务器	DELL R910	4	维保服务、备品备件库服务	区域卫生数据中心	7*24
27	虚拟带库	EMC DD640	1	维保服务、备品备件库服务	区域卫生数据中心	7*24
28	存储	DELL 存储 MD3600f	1	维保服务、备品备件库服务	区域卫生数据中心	7*24
29	服务器	IBM X3650 M4	1	维保服务、备品备件库服务	区域卫生数据中心	7*24
30	负载均衡	Array APV 4600	1	维保服务、备品备件库服务	区域卫生数据中心	7*24
31	外网核心交换机	华为 9706	1	维保服务、备品备件库服务	区域卫生数据中心	7*24
32	楼层交换机	华为 5748	19	维保服务、备品备件库服务	区域卫生数据中心	7*24
33	双活数据复制容灾设备	EMC VPLEX	1	维保服务、备品备件库服务	区域卫生数据中心	7*24

2.4.2 安全产品清单

序号	系统名称	设备型号	数量	服务方式和内容	服务范围	服务级别	备注
1	奇安信网神数据库审计与防护系统 V6.0	K6000-H-TF10P	3	维保服务、备品备件库服务	区域卫生数据中心	7*24	需提供原厂售后服务承诺函
2	网神 Sec IDS 3600 入侵检测系统 V40	D5000-TG2M	1	维保服务、备品备件库服务	区域卫生数据中心	7*24	需提供原厂售后服务承诺函

3	天融信数据库安全网关系统 V3	TDSM-DBGW	2	维保服务、备品备件库服务	区域卫生数据中心	7*24	
4	天融信防火墙系统 V3	NGFW4000-UF	3	维保服务、备品备件库服务	区域卫生数据中心	7*24	
5	美创数据脱敏	DM-G10SH	1	维保服务、备品备件库服务	区域卫生数据中心	7*24	需提供原厂售后服务承诺函
6	美创库防水坝	DW-G30SH	1	维保服务、备品备件库服务	区域卫生数据中心	7*24	需提供原厂售后服务承诺函
7	深信服防火墙	AF-1000-B1180	16	维保服务、备品备件库服务	区域卫生数据中心及区属医疗机构	7*24	需提供原厂售后服务承诺函
8	日志收集与分析系统	网神 SecFox R2000-T1624	1	维保服务、备品备件库服务	区域卫生数据中心	7*24	需提供原厂售后服务承诺函
9	堡垒机	天融信 TopSAG	1	维保服务、备品备件库服务	区域卫生数据中心	7*24	
10	社区医院专网	网神	1	维保服	区域	7*24	需提供

	防火墙	SecGate3600-A1500		务、备品备件库服务	卫生数据中心		原厂售后服务承诺函
11	社区医院专网IPS	网神 SecIPS3600 入侵防御系统	1	维保服务、备品备件库服务	区域卫生数据中心	7*24	需提供原厂售后服务承诺函
12	防毒墙	天融信 TF51338-VIRUS	1	维保服务、备品备件库服务	区域卫生数据中心	7*24	
13	边界防火墙	360 网神天堤防火墙 NSG3000-TE45	1	维保服务、备品备件库服务	区域卫生数据中心	7*24	需提供原厂售后服务承诺函
14	服务器区域防火墙 1	360 网神防火墙系统 NSG5000-TG30	2	维保服务、备品备件库服务	区域卫生数据中心	7*24	需提供原厂售后服务承诺函
15	互联网区域网络 VPN	安达通 JJ1207B+	1	维保服务、备品备件库服务	区域卫生数据中心	7*24	需提供原厂售后服务承诺函
16	外网隔离防火墙	深信服 AF-1000-B1180	1	维保服务、备品备件库服务	区域卫生数据中心	7*24	需提供原厂售后服务承诺函
17	外网出口防火墙	网神 SecGate 3600 G30-HWS66	1	维保服务、备品备件库服务	区域卫生数据中心	7*24	需提供原厂售后服务承诺函
18	政务外网边界	网神 SecGate3600	1	维保服务、备品	区域卫生	7*24	需提供原厂售

	防火墙	A1500-T150P		备件库服务	数据中心		后服务承诺函
19	政务外网接入防火墙	网神 SecGate3600 A3000-T550M	1	维保服务、备品备件库服务	区域卫生数据中心	7*24	需提供原厂售后服务承诺函

2.4.3 响应时间和服务要求

1. 热线电话支持：提供全年24小时电话技术支持。
2. 设备返修维修支持：报障响应时间30分钟内，提供每周7天×24小时的设备返修维修支持服务，在接到设备维修电话后，在4小时内派遣工程师至现场处理维修。
3. 备品备件：提供备品备件服务。

2.5 机房环境监控维保部分

序号	分类	维护内容	服务方式和内容	续保年限
1.	机房环境监控	机房环境监控运维	故障响应、定期日志维护	一年

2.5.1 响应时间和服务要求

1. 热线电话支持：提供全年24小时电话技术支持，报障响应时间30分钟内。
2. 远程技术支持：提供远程故障诊断处理服务。要求5×8小时受理。
3. 电子化支持：提供全年24小时的在线方式的WEB网站技术支持。

第 3 章　运维服务管理要求

本项目运维服务商应满足并达到以下要求。

3.1 运维服务商职责

在本项目中，运维服务商作为整体运维服务的提供方，承担运维服务的技术管理、实施和协调工作。包括 ：

1. 制定切实可行的维保计划，提供本招标书所要求的相关服务；

2. 提供合格的技术人员，来保证项目的顺利实施；

3. 提供完整的技术文档资料、完整的测试、调优、维护建议；

4. 在服务期内持续进行系统的优化和良好的技术支持；

5. 配合招标方相关软件、硬件的安装、测试、升级和调优等工作；

6. 在维保服务期内，若系统发生突发事件，提供恢复系统的临时软硬件设备，及时恢复系统运行。

3.2 运维服务体系

运维服务商应提交正式的文件，说明其具备专业的支持服务管理机构，管理流程和服务保障体系。运维服务商应配备专业的服务响应中心，能够7*24小时响应招标方的服务请求，并具有流程化的管理处理能力。

3.3 运维团队构成

为完成本项目，响应人应组建项目小组，在提交的投标文件中需明确项目组成员。运维服务商在组建运维技术团队时,必须满足以下要求：

本项目项目经理需具备PMP项目经理资质与CISP安全认证；团队技术驻场人员具备CISP安全认证、CISAW安全运维或同等级、安全等设备维护能力和技术, 工作时间与长宁卫健委办公人员的工作时间一致。并提供二线技术支持团队，团队成员（以下岗位可兼职）包括：项目经理、运维工程师等，提供故障解决方案和咨询服务，紧急情况下进驻现场提供服务。

本项目运维团队人员不少于三人。

响应人在中标后，应认真组织好技术及管理队伍，做好运维工作。维护期内原则上不允许更换项目技术人员。维护期间确需人员变动，须配备同资质人员，并提前一个月报请招标方认可。

3.4 现场支持管理

遵守招标方的管理制度要求。提供现场支持服务，统一接受用户的服务请求，现场支持服务作为系统运维的统一入口，统一接受用户服务请求。要求运维服务商负责现场支持中心服务工作，配备提供人员驻场，负责协调系统软硬件维护，以及保障长宁卫健委业务正常运行等工作。

同时，运维服务商应为本项目成立二线技术支持团队，负责协助一线人员，为本项目提供高层次技术支持和重大事项处理服务。

3.5 设备维护管理

为确保业务系统软硬件设备的正常可用，运维服务商对系统运行支撑环境和系统运行平台中的各类硬件设备进行常规性例行的检查，在每次维保服务完成后，应在及时提交《系统运行维护记录》，包括故障原因分析、处理过程、维护建议等。运维服务商按月向招标方报送《系统运行状况月度报告》、按季向招标方报送《系统巡检报告》、每年向招标方提供《年度维护报告》。

3.6 信息系统监控管理

为确保信息系统的可用性和连续性，运维服务商应提供主动发现问题、排除故障的服务，从应用层面检查各业务应用，主动发现问题，保障业务的可持续性。

3.7 安全服务管理

运维服务商必须服从招标方对安全管理规定和要求，配合落实安全管理的各项工作，提供技术保障服务。

3.8 资产管理

在运维服务期间，运维服务商有责任保证信息系统在线资产的完整、可用，并协助招标方提供系统资源管理、服务。

3.9 信息保密制度

运维服务商对本项目维护服务内容有保守秘密的义务，需要做到以下几点：

1. “保密信息”是指长宁卫健委在履行本合同中提供或传授给供应商人员，或者供应商人员在履行本合同中知晓的信息，无论是口头或书面形式、无论是否标明保密或拥有所有权，包括但不限于专利、版权、商业秘密、专有技术、专有信息、技巧、草图、绘图、模型、发明、工序、规则系统（算法）、软件程序、软件资料，硬件信息和应用程序接口等任何技术和非技术的信息；也指与现有、未来和预计的产品和服务相关的任何方案，包括但不限于研发、设计、规格、工程、财务、采购、生产、客户表、市场预测和销售等信息。
2. 供应商同意对保密信息予以保密；未经长宁卫健委事先书面同意，在任何情况下都不泄露或披露保密信息；履行期限届满后，不保留任何保密信息的原件，复印件和电子信息。供应商不得向任何第三方透露任何或部分保密信息。供应商不得将长宁卫健委透露的任何保密信息用于执行合同以外的事务。
3. 未经长宁卫健委同意，供应商不得在广告或任何公开材料或活动中使用长宁卫健委的名称。
4. 如果供应商应政府机构、法院或其它经授权的官方部门的要求公布该保密信息，供应商同意及时通知长宁卫健委以便长宁卫健委对此提出异议或获取保护令。供应商应采用一切措施保护保密资料。
5. 供应商违反本协议规定向任何第三方透露保密信息，应承担违约责任，并赔偿长宁卫健委因此受到的损失。
6. 本条的上述义务，在合同终止后将继续有效三年。

第 4 章　运维服务技术要求

4.1　服务要求

4.1.1　系统数据保密要求

负责遵守职业道德，确保系统及业务数据不会因运维服务商原因外泄，如发生以上问题，运维服务商必须承担全部法律责任。

4.1.2　系统及数据安全要求

负责在实施服务的过程中提供完善的工作内容说明及操作步骤，并通过备份等方法确保系统及数据不被损坏或能及时恢复，如发生以上问题，承担全部法律责任。

4.1.3　电话支持服务

运维服务商应设立热线响应电话，并安排有经验的工程师接受申报。当设备出现故障时，招标方通过运维服务商指定的热线响应电话进行故障报修或技术咨询。电话支持的响应时间为7*24小时。

4.1.4　现场支持服务

运维服务商提供现场支持服务时，应安排具有相关专业技术能力的工程师赴现场分析故障原因，制定故障解决方案，并最终排除故障。现场支持的响应时间为7*24小时。

运维服务商的技术人员在处理故障时不能影响到其他设备的正常运行；在必须进行系统重装或系统启动等较大操作时，须经招标方相关主管批准后方可实施。

运维服务商服务人员在处理故障时，要认真填写《故障处理报告》，并需得到用户签字确认及存档后方可离开，《故障处理报告》同时存入运维服务商的用户故障处理数据库（知识库）。

负责在服务过程中遵守规章制度，并根据要求，提供以下说明材料：

1. 提供工作内容、操作方法；

2. 风险分析及风险应对承诺签字；

3. 操作者姓名；

4. 需要软件商配合事项；

4.1.5 备品备件服务

当设备出现故障，运维服务商确认故障部件后，协调设备提供商发出替换备件（不另行收取费用），而不必等待坏损设备退回设备提供商，使得在最快时间内排除故障，避免严重后果和业务长时间中断。

4.1.6 故障级别与服务响应速度、故障恢复时间要求

当招标方的设备发生问题时，根据招标方对故障的定级，运维服务商需提供不同的响应速度及故障恢复时间。

故障级别定义：

- 一级：现有的系统停机，或造成业务中断或数据丢失。
- 二级：现有系统的可操作性严重降级，或由于系统性能降低严重影响业务运作。
- 三级：系统可操作性受损，但业务运作仍可正常工作。
- 四级: 系统功能、安装或配置方面需要改进，但明显对业务运作影响度低，或根本没有影响。

维护方在接到故障报告后，10分钟内给出口头应急措施，1小时内给出完整解决方案。一级故障或二级故障，在电话或其他即时通讯软件无法提供解决办法的情况下，尽可能在应急措施后先恢复网络正常，并在45分钟内赶赴现场处理。三级故障和四级故障一般以远程支持的方式解决，由于产品本身原因无法解决的，维护方需要在两天内赶赴现场负责处理。

- 第一级（紧急故障）：

当核心设备或系统发生严重故障导致业务瘫痪时，服务商需立即响应（定义为30分钟内），并确保工程师2小时内到达现场，6小时内恢复系统。

- 第二级（重要故障）：

当系统出现严重故障，部分服务异常但系统仍可运行时，服务商需在2小时内响应，并派遣工程师进行现场维护。

- 第三级（次要故障）：

当系统个别服务异常但不影响整体运行时，服务商需在4小时内响应，并派遣工程师进行现场维护。

- 第四级（一般问题）：

对于不影响系统正常运行的一般性问题，服务商需通过电话或远程方式进行支持，或在24小时内安排现场服务以排除故障。

要求故障处理结束后2个工作日内，提交《故障处置工作小结》。

4.2 服务报告要求

负责提供以下报告：

报告	内容	时间
日常巡检记录	记录每日驻场巡检信息	每日更新
月度巡检报告	总结本月的巡检结果	1 次/月，下月 5 日内提交
季度巡检报告	总结本季度的巡检结果	1 次/季度，下月 5 日内提交
服务年报告	总结全年的工作情况和资源使用情况	1 次/年，年后 10 日内提交
重大事件服务报告	总结重要事件的服务情况	重大故障发生的下一工作日提交

4.3 技术支撑服务

4.3.1 现场设备检查服务

现场设备检查服务要求包括：

1. 巡检工作应有相关记录，并形成工作小结，涉及整改内容的需在规定时间内完成整改方案，并提交整改结果报告。

2.运维服务商需为招标方建立设备维修档案，并根据设备运行情况向招标方提供设备升级、改造、更换的建议和方案。

3. 多厂商多平台技术支持服务

根据招标方运维服务要求，如需原厂商或第三方服务机构提供技术支持的，运维服务商应能够为招标方提供多厂商多平台技术协作支持（包括主机、存储等）。

4.3.2 安全维护服务支持要求

安全维护服务支持要求包括：

1. 日常安全监测、监控。安全相关设备的状态及日志分析；安全配置、策略优化、备份。安全相关设备、相关系统的配置、策略优化及定期备份工作。

2. 安全事件处置及应急响应。当出现安全事件时，及时协调包括运维服务商技术团队、原厂技术支持在内的多方资源进行事件处理，同时根据安全事件级别启动应急响应相关应急预案。

4.4 技术文档要求

4.4.1 系统维护档案管理

运维服务商应配备专人负责系统维护档案的管理。建立维护档案版本管理、文档规范管理等制度。维护档案内容包括，设备详细配置清单、所使用的操作系统、软件系统版本号、系统的使用情况及系统的配置参数等。

4.4.2 技术文档清单

运维服务商需定期提交以下技术文档。

序号	工作产出	提交频度	备注
1.	系统运行维护记录	不定期	包括运维基本情况、故障处理记录、系统备份记录、系统升级记录
2.	故障处置工作小结	不定期	
3.	IT 突发事件/故障处理报告	不定期	
4.	系统应急响应操作	不定期	

	记录		
5.	年度运维总报告	每年一次	
6.	故障案例分析报告	不定期	

4.5 其他运维服务要求

4.5.1 一般要求

1. 供应商在本地有固定的售后服务团队。
2. 供应商应本着认真负责的态度，组织技术队伍，认真做好服务维护工作。
3. 供应商必须提供服务实施计划，经用户方同意后，严格执行。

4.5.2 其他资质要求

1. 供应商需具有运行维护货物的原始厂商服务授权。
2. 投标人具有CNCERT国家互联网应急中心网络安全应急服务支撑单位证书。
3. 投标人具有CCRC信息安全服务资质认证证书（信息系统安全运维服务二级或以上）、CCRC信息安全服务资质认证证书（信息系统安全集成三级或以上）、CCRC信息安全服务资质认证证书（信息安全应急处理二级或以上）、CCRC信息安全服务资质认证证书（信息安全风险评估一级）。
4. 投标人具有ISO9001质量管理体系认证证书、ISO20000信息技术服务管理体系认证证书、ISO27001信息安全管理体系认证证书。

4.5.3 人员培训

1. 供应商应负责对使用人员进行培训及考核，保证技术人员能够正常使用相关设备。
2. 供应商应在投标文件中提供详细的培训计划和培训课程。

4.5.4 重要保障服务

根据招标方特定时间段的工作需要，运维服务商应向招标方提供相关重要保障服务。重要保障服务，包括汛期、重大节假日、国家军事或政治活动等期间的系统运行服务保障工作。

第 5 章　信息安全要求

对于原有通过信息安全等级保护三级水平评测的系统，响应人提供的运维服务需达到信息安全等级保护三级水平的要求，同时具备区域卫生信息系统承建能力及软硬件安全等保服务能力厂商，需提供相关合同及资质证明。

第 6 章　售后服务要求

1. 供应商在本地应设立分公司或常驻售后技术支持服务机构。
2. 维护内容包括定期预防性维护、定期优化改进维护、应急故障维护。
3. 要求供应商提供5*8常驻现场服务，未经用户方同意成交供应商不得随意变更现场服务人员。
4. 对于本次要求的硬件设备维护，供应商需要根据巡检情况提交系统运行报告。

第 7 章　其他要求

1. 供应商提供的服务，如涉及产品升级、设备更换扩展时不应改变整个系统的结构、通信方式、管理模式，不应破坏应用软件的正常工作环境。
2. 供应商应该保证所提供的所有产品或服务皆不侵犯任何第三方的版权、知识产权和其他合法权利。
3. 业主有权根据本项目应用需求和预算情况，在有关规定的范围内增减上述所购买服务产品的数量和配置。
4. 供应商必须根据上述服务要求和服务响应时间作出无推诿承诺。
5. 响应人应在投标书中详细列出服务项目清单，对每项服务，需明确服务提供方名称、服务内容、服务方式、服务人员技术要求以及服务响应时

间等。所有服务费用单列，计入投标总价。

第 8 章　付款方式

进度	乙方应向甲方提交的资料	进度款的支付
合同签订后	发票	合同签订后 15 个日历天内，向乙方支付合同价的 50%；
	发票	运维服务到期经甲方确认合格后 15 个日历天内，向乙方支付合同价的 50%。

如出现逾期支付相关费用等情况，采购人将支付中标单位相应利息；如对中标单位造成损失的，依法给予中标单位相关补偿。