

采购需求书

包 1：数据中心服务器维保服务要求

1、维护的要求和期限

(1) 提供软、硬件基本维保服务，包含但不限于提供服务器、服务器虚拟化系统的现场技术服务，硬件备件现场更换服务，软、硬件版本升级现场服务，核心设备故障排错及恢复业务服务等，确保能迅速解决采购人核心业务网设备故障、排除运行隐患，保证采购人各项业务的稳定运行。为确保设备兼容性与技术支持连续性，投标人需提供原厂可溯源的维保服务。如提供非原厂服务，须提供原厂授权证明及同等质量的技术保障承诺，经采购人书面确认后方可实施。

(2) 维护期限：3年。

2、维护工作范围

★(1) 投标人为采购人服务器、服务器虚拟化系统提供3年产品原厂可溯源维保服务；服务标准为7*24小时级别，参保设备维护期限为3年，自合同签订之日起。

#(2) 中标后投标人应提供维保清单内具有满足本项目采购需求的售后服务证明文件，包括但不限于售后服务承诺函或授权函等。

(3) 负责本次招标所有系统设备的技术支持和运行维护工作。

3、维护工作内容和标准

总体描述：客户服务经理与支持团队、快速备件更换、现场技术支持、维护性软件版本支持以及网站支持等内容。能够有效帮助采购人技术支持人员维护网络稳定运行，满足采购人对高效、稳定的网络环境的需求。

(1) 服务器、服务器虚拟化系统参保须为原厂可溯源保修：中标公司需确保采购人所要求维保服务清单内软、硬件设备故障保修为原厂可溯源保修或备件更换。

(2) 客户服务经理与支持团队：在设备维保期内，投标人须指定专责服务主管、专责工程师团队、专职项目经理，项目经理的更换须得到采购人同意。

★(3) 快速备件先行更换服务：投标人应向采购人提供及时周到的原厂可溯源快速备件更换服务。服务标准为备件先行7*24响应。

一旦定位是硬件故障，中标人应在规定时间内将原厂可溯源正品备件先行运抵现场，保证故障部件得到及时更换，以使采购人的业务能在最短时间内恢复正常。

#(4) 工程师快速现场支持服务：考虑到采购人信息系统组网复杂，业务重要，且设备均为高端产品，在业务出现问题或者设备出现问题时，需要及时排查并能迅速解决，故此，投标人应承诺在重大法定节假日、重大接入网故障事件，重要切换、上线、变更、切换演练等大型网络变动时提供现场技术支持服务。具体内容包括但不限于：

- A. 工程师快速现场支持到达现场支持;
- B. 现场备件更换支持服务;
- C. 现场故障诊断及故障排除;
- D. 现场软件升级。

投标人工程师及投标人安排的原厂可溯源技术支持工程师，自接到首次现场支持通知（电话、短信、微信等）时起，到达指定现场的时间要求为1小时内。首次通知无响应的（包括但不限于电话不接或挂断、短信不回复、微信不回复等，以采购人定义为准），均视为通知已到达并开始计算时限，如不能按时（1小时内）抵达现场，每次处以2000元人民币罚款。一年服务期内，累计超过3次不能按时抵达现场的情况，采购人有权终止合作及合同履行，并终止支付合同款项且不承担任何相关责任。

技术支持具体响应时间定义如下：

P1级故障——设备在运行故障中出现整机系统瘫痪或服务中断，导致设备的基本功能不能实现或全面退化的故障。故障确诊时间：1小时，故障排除时间≤8小时。

P2级故障——设备在运行中出现的故障具有潜在的系统瘫痪或服务中断的危险，并可能导致设备的基本功能不能实现或全面退化。故障确诊时间：3小时，故障排除时间≤6小时。

P3级故障——设备在运行中出现影响业务，并导致系统性能或服务部分退化的故障。故障确诊时间：12小时，故障排除时间≤6小时。

P4级故障——咨询类问题或设备在运行安装过程中，客户对产品功能配置等方面需要的信息和需求，对业务系统影响极小。故障确诊时间：24小时，故障排除时间≤6小时。

（5）远程技术支持服务

投标人应提供7*24的服务热线，由专门受理客户问题的维护团队提供全天候不间断的产品技术咨询、故障申报受理、硬件维修受理、以及服务政策咨询等服务内容。

（6）维护性软件版本支持服务

在服务有效期内，投标人应协调原厂公司向客户提供其所购设备的管理软件（如HPE iLO、H3C CAS等）的维护性版本及升级版本，如：BUG修补文件，新版本的主机软件，以及该软件配套的文档资料。获得软件后，客户将享有与原有软件相同的许可权利，但不得用于商业目的的传播。

具有特殊功能并单独销售的主机软件不在提供范围内。进行License控制与销售的软件产品，如网管软件、计费软件等，只提供软件补丁，不提供新的License或新版本的软件本身。

（7）应急响应

服务类型：不定期服务

服务说明：为采购人信息系统平台提供重大安全事故和突发网络安全事件的应急响应服务。在采购人院区网络系统发生业务瘫痪、网络入侵等重大安全事故时，提供现场应急技术

支持。

要求投标人30分钟内应急响应、1小时内安全技术专家到达现场处理问题、2小时内提出安全解决方案。由于硬件设备等原因不能立即解决的，提供临时解决方案建议，最大限度地保证采购人业务的正常运行。同时由投标人协调联系相关设备厂商，以保证尽快解决问题。

(8) 巡检服务

原厂可溯源技术支持工程师定期巡检服务（至少每个季度一次），对设备的运行状态进行检查和分析，提交正式服务报告。原厂可溯源技术支持工程师定期性能分析服务（至少每个季度一次），提供设备性能、高可用评估的季度分析报告，以便采购人了解维护状况，及时预见并解决问题。

(9) 重大项目现场支持

配合重大项目实施工作。根据采购人的需要，在有关项目实施中，配合完成所保设备的搬迁、系统安装调整等工作。

4、人员工作要求

投标人中标后，指定一名客户代表，制定服务计划，联系服务资源，定期与采购人技术人员交流，对维护情况进行回顾，组织和协调服务事宜，并提交阶段性服务报告。投标人技术人员按照合同要求进行服务，在现场服务时要听从采购人相关人员的安排。

5、内网准入工作

投标人所有提供服务的相关工程师及工作人员的办公电脑需配合采购人做好内网电脑入网、受控。

6、报价说明

投标人报出总价应保证其报价的充分性、完整性和符合性，以及根据自身实力所报出具有竞争力的综合取费。采购人不统一组织投标人对工程现场和其周围环境进行考察。投标人根据自身需要，确定是否自行对现场和其周围环境进行考察，以获取编制投标文件和签署实施工程所需的各项资料，及做出自己的判断和估价，并在投标时充分考虑上述因素。一旦中标后，投标人不得以不了解现场情况为由，提出任何形式的增加项目价款或索赔要求。投标人须承担现场考察的责任和风险，踏勘所发生的费用由投标人自行承担。

7、驻场人员要求

服务期内，投标人需要提供 1 名工程师进行驻场服务。驻场工程师要求有三年以上 IT 设备运维工作经验，具备厂商中级及以上认证证书（或具有同等能力水平）。具体工作包括以下内容：

A. 日常设备维护。精通数据中心常见服务器（如 HPE、新华三、华为、联想、浪潮等）设备的日常运维、巡检、故障定位与处置能力，精通服务器虚拟化软件 CAS、VMware 的日常

运维、巡检、故障定位与处置能力，具备本次招标涉及的设备及系统的日常运维能力，必要时能够进行调整和优化，保障平台正常运行；

B. 补丁、版本升级服务。能够对数据中心各项服务器及虚拟化系统进行软件补丁、版本升级，使数据中心各项设备处于良好运行状态；

C. 故障处理。预警并协助数据中心预防重大故障的发生，在发生故障时可以快速解决故障；

D. 保障服务。为了保障重大节日期间机房软硬件支撑环境安全运行，向采购人提供现场工程师值守服务，并在保障结束后提供服务总结报告和建议；

E. 其他现场技术支持服务。包括相关技术咨询、新需求的配合解决、配合割接实施等其他现场技术支持服务；

F. 驻场工程师按采购人作息时间上下班，办公场地由采购人提供。

8、维保服务清单

序号	设备名称	设备型号	产品描述	数量
1	刀片服务器机箱	Bladesystem C7000	HPE BLc7000 1PH 2PS 4Fan Tr1 IC Plat Encl	2
2	虚拟化服务器	BL460c	HPE BL460c 刀片式服务器	30
3	管理服务器	BL460c	HPE BL460c 刀片式服务器	2
4	服务器虚拟化系 统	VC-CAS-ENT	功能模块-H3C CAS-VCAM8CAS-CAS 云计 算管理平台-纯软件(DVD)-国内版	1
		LIS-CAS-CVMA-E NT-2	License 授权函-H3C CAS-VCAM8CVMA-CVM 虚拟化管理系统企 业版软件 License 费用-管理 2 个物理 CPU-国内版	30
5	HIS 业务备份服 务器	DL580 Gen9	HPE DL580 GEN9 服务器	2
6	日志采集与分析 系统	RS-FD4530-21SF F-ITOA	装配组件-H3C FlexData 4530-RSBZ1FD4530-4U 服务器-国内海 外合一版	1
7	关键业务数据库 服务器	Superdome X	HPE Superdome X Base Enclosure	2
8	智慧财务系统服 务器	R6900 G3	H3C R6900 G3 服务器	3

包 2：数据中心存储系统维保服务要求

1、维护的要求和期限

(1) 提供软、硬件基本维保服务，包含但不限于提供备份系统、备份设备、存储系统、存储交换机的现场技术服务，硬件备件现场更换服务，软、硬件版本升级现场服务，核心设备故障排错及恢复业务服务等，确保能迅速解决采购人核心业务网设备故障、排除运行隐患，保证采购人各项业务的稳定运行。为确保设备兼容性与技术支持连续性，投标人需提供原厂可溯源的维保服务。如提供非原厂服务，须提供原厂授权证明及同等质量的技术保障承诺，经采购人书面确认后方可实施。

(2) 维护期限：自合同签订之日起3年。

2、维护工作范围

★ (1) 投标人为采购人备份系统、备份设备、存储设备提供 3 年产品原厂可溯源维保服务；服务标准为 7*24 小时级别，参保设备、系统维护期限为 3 年，自合同签订之日起。

(2) 中标后投标人应提供维保清单内具有满足本项目采购需求的售后服务证明文件，包括但不限于售后服务承诺函或授权函等。

(3) 负责本次招标所有系统设备的技术支持和运行维护工作。

3、维护工作内容和标准

总体描述：客户服务经理与支持团队、快速备件更换、现场技术支持、维护性软件版本支持以及网站支持等内容。能够有效帮助采购人技术支持人员维护网络稳定运行，满足采购人对高效、稳定的网络环境的需求。

(1) 备份系统、备份设备、存储设备参保须为原厂可溯源保修：中标人需确保采购人所要求维保服务清单内软、硬件设备故障保修为原厂可溯源保修或备件更换。

(2) 客户服务经理与支持团队：在设备维保期内，投标人须指定专责服务主管、专责工程师团队、专职项目经理，项目经理的更换须得到采购人同意。

★ (3) 快速备件先行更换服务：投标人应向采购人提供及时周到的原厂可溯源快速备件更换服务。服务标准为备件先行7*24响应。

一旦定位是硬件故障，中标人应在规定时间内将原厂可溯源正品备件先行运抵现场，保证故障部件得到及时更换，以使采购人的业务能在最短时间内恢复正常。

(4) 工程师快速现场支持服务：考虑到采购人信息系统组网复杂，业务重要，且设备均为高端产品，在业务出现问题或者设备出现问题时，需要及时排查并能迅速解决，故此，投标人应承诺在重大法定节假日、重大接入网故障事件，重要切换、上线、变更、切换演练等大型网络变动时提供现场技术支持服务。具体内容包括但不限于：

A. 工程师快速现场支持到达现场支持；

B. 现场备件更换支持服务；

C. 现场故障诊断及故障排除；

D. 现场软件升级。

投标人工程师及投标人安排的原厂可溯源技术支持工程师，自接到首次现场支持通知（电话、短信、微信等）时起，到达指定现场的时间要求为1小时内。首次通知无响应的（包括但不限于电话不接或挂断、短信不回复、微信不回复等，以采购人定义为准），均视为通知已到达并开始计算时限，如不能按时（1小时内）抵达现场，每次处以2000元人民币罚款。一年服务期内，累计超过3次不能按时抵达现场的情况，采购人有权终止合作及合同履行，并终止支付合同款项且不承担任何相关责任。

技术支持具体响应时间定义如下：

P1级故障——设备在运行故障中出现整机系统瘫痪或服务中断，导致设备的基本功能不能实现或全面退化的故障。故障确诊时间：1小时，故障排除时间≤8小时。

P2级故障——设备在运行中出现的故障具有潜在的系统瘫痪或服务中断的危险，并可能导致设备的基本功能不能实现或全面退化。故障确诊时间：3小时，故障排除时间≤6小时。

P3级故障——设备在运行中出现影响业务，并导致系统性能或服务部分退化的故障。故障确诊时间：12小时，故障排除时间≤6小时。

P4级故障——咨询类问题或设备在运行安装过程中，客户对产品功能配置等方面需要的信息和需求，对业务系统影响极小。故障确诊时间：24小时，故障排除时间≤6小时。

（5）远程技术支持服务

投标人应提供7*24的服务热线，由专门受理客户问题的维护团队提供全天候不间断的产品技术咨询、故障申报受理、硬件维修受理、以及服务政策咨询等服务内容。

（6）维护性软件版本支持服务

在服务有效期内，投标人应协调原厂公司向客户提供其所购设备主机软件的维护性版本及升级版本，如：BUG修补文件，新版本的主机软件，以及该软件配套的文档资料。获得软件后，客户将享有与原有软件相同的许可权利，但不得用于商业目的的传播。

具有特殊功能并单独销售的主机软件不在提供范围内。进行License控制与销售的软件产品，如网管软件、计费软件等，只提供软件补丁，不提供新的License或新版本的软件本身。

（7）应急响应

服务类型：不定期服务

服务说明：为采购人信息系统平台提供重大安全事故和突发网络安全事件的应急响应服务。在采购人院区网络系统发生业务瘫痪、网络入侵等重大安全事故时，提供现场应急技术支持。

要求投标人30分钟内应急响应、1小时内安全技术专家到达现场处理问题、2小时内提出安全解决方案。由于硬件设备等原因不能立即解决的，提供临时解决方案建议，最大限度地

保证采购人业务的正常运行。同时由投标人协调联系相关设备厂商，以保证尽快解决问题。

(8) 巡检服务

原厂可溯源技术支持工程师定期巡检服务（至少每个季度一次），对设备的运行状态进行检查和分析，提交正式服务报告。原厂可溯源技术支持工程师定期性能分析服务（至少每个季度一次），提供设备性能、高可用评估的季度分析报告，以便采购人了解维护状况，及时预见并解决问题。

(9) 重大项目现场支持

配合重大项目实施工作。根据采购人的需要，在有关项目实施中，配合完成所保设备的搬迁、系统安装调整等工作。

4、人员工作要求

投标人中标后，指定一名客户代表，制定服务计划，联系服务资源，定期与采购人技术人员交流，对维护情况进行回顾，组织和协调服务事宜，并提交阶段性服务报告。投标人技术人员按照合同要求进行服务，在现场服务时要听从采购人相关人员的安排。

5、内网准入工作

投标人所有提供服务的相关工程师及工作人员的办公电脑需配合采购人做好内网电脑入网、受控。

6、报价说明

投标人报出总价应保证其报价的充分性、完整性和符合性，以及根据自身实力所报出具有竞争力的综合取费。采购人不统一组织投标人对工程现场和其周围环境进行考察。投标人根据自身需要，确定是否自行对现场和其周围环境进行考察，以获取编制投标文件和签署实施工程所需的各项资料，及做出自己的判断和估价，并在投标时充分考虑上述因素。一旦中标后，投标人不得以不了解现场情况为由，提出任何形式的增加项目价款或索赔要求。投标人须承担现场考察的责任和风险，踏勘所发生的费用由投标人自行承担。

7、维保服务清单

序号	设备名称	设备型号	产品描述	数量
1	备份系统	CB	H3C CB 备份软件	1
2	备份设备	Storeonce 5100	HPE StoreOnce 5100 48TB	2
3	存储设备	3PAR 8450	HPE 3PAR 8450 4N+SW Storage Field Base	2
4	存储设备	3PAR 8200	HPE 3PAR 8200 2N+SW Storage Field Base	3
5	备份设备	MSL4048	HP MSL4048 物理带库	1
6	存储设备	3PAR 8440	HPE 3PAR 8440	1
7	存储设备	CF8820	H3C CF8820	1
8	存储设备	MSA2040	MSA2040 存储设备	1

9	存储设备	CF8850H	外网信创存储 H3C ST-CF8850H-24LFF-512G	1
10	存储设备	CF8850H	内网信创存储 H3C ST-CF8850H-24LFF-512G、 ST-CF8850H-DEL-24LFF*2	1
11	存储设备	UniStorX10516 G3	超融合存储 H3C UniStorX10516 G3	3
12	存储设备	5110 V5	华为存储 5110 V5 Enhanced	2
13	存储交换机	SNS2624	华为存储光纤交换机 SNS2624	2
14	存储交换机	SN6000B	SN6000B 光交换机	4

包 3：安全维保服务要求

1、维护的要求和期限

(1) 提供软、硬件基本维保服务，包括但不限于提供安全设备、系统技术现场服务，硬件备件更换现场服务，软、硬件版本升级现场服务，核心设备故障排错及恢复业务服务等，确保能迅速解决采购人核心业务网设备故障、排除运行隐患，保证采购人各项业务的稳定运行。为确保设备兼容性与技术支持连续性，投标人需提供原厂可溯源的维保服务。如提供非原厂服务，须提供原厂授权证明及同等质量的技术保障承诺，经采购人书面确认后方可实施。

(2) 维护期限：自合同签订之日起3年。

2、维护工作范围

★(1) 投标人为采购人安全设备、系统提供 3 年产品原厂可溯源维保服务、3 年特征库升级服务；服务标准为 7*24 小时级别，参保设备维护期限为 3 年，自合同签订之日起。

#(2) 中标后投标人应提供维保清单内具有满足本项目采购需求的售后服务证明文件，包括但不限于售后服务承诺函或授权函等。

(3) 负责本次招标所有系统设备的技术支持和运行维护工作。

3、维护工作内容和标准

总体描述：客户服务经理与支持团队、快速备件更换、现场技术支持、维护性软件版本支持以及网站支持等内容。能够有效帮助采购人技术支持人员维护网络稳定运行，满足采购人对高效、稳定的网络环境的需求。

(1) 安全设备、系统参保须为原厂可溯源保修：中标人需确保采购人所要求维保服务清单内软、硬件设备故障保修为原厂可溯源保修或备件更换。

(2) 客户服务经理与支持团队：在设备维保期内，投标人须指定专责服务主管、专责工程师团队、专职项目经理，项目经理的更换须得到采购人同意。

★(3) 快速备件先行更换服务：投标人应向采购人提供及时周到的原厂可溯源快速备件更换服务。服务标准为备件先行7*24响应。

一旦定位是硬件故障，中标人应在规定时间内将原厂可溯源正品备件先行运抵现场，保证故障部件得到及时更换，以使采购人的业务能在最短时间内恢复正常。

#(4) 工程师快速现场支持服务：考虑到采购人信息系统组网复杂，业务重要，且设备均为高端产品，在业务出现问题或者设备出现问题时，需要及时排查并能迅速解决，故此，投标人应承诺在重大法定节假日、重大接入网故障事件，重要切换、上线、变更、切换演练等大型网络变动时提供现场技术支持服务。具体内容包括但不限于：

- A. 工程师快速现场支持到达现场支持；
- B. 现场备件更换支持服务；
- C. 现场故障诊断及故障排除；

D. 现场软件升级。

投标人工程师及投标人安排的原厂可溯源技术支持工程师，自接到首次现场支持通知（电话、短信、微信等）时起，到达指定现场的时间要求为1小时内。首次通知无响应的（包括但不限于电话不接或挂断、短信不回复、微信不回复等，以采购人定义为准），均视为通知已到达并开始计算时限，如不能按时（1小时内）抵达现场，每次处以2000元人民币罚款。一年服务期内，累计超过3次不能按时抵达现场的情况，采购人有权终止合作及合同履行，并终止支付合同款项且不承担任何相关责任。

技术支持具体响应时间定义如下：

P1级故障——设备在运行故障中出现整机系统瘫痪或服务中断，导致设备的基本功能不能实现或全面退化的故障。故障确诊时间：1小时，故障排除时间≤8小时。

P2级故障——设备在运行中出现的故障具有潜在的系统瘫痪或服务中断的危险，并可能导致设备的基本功能不能实现或全面退化。故障确诊时间：3小时，故障排除时间≤6小时。

P3级故障——设备在运行中出现影响业务，并导致系统性能或服务部分退化的故障。故障确诊时间：12小时，故障排除时间≤6小时。

P4级故障——咨询类问题或设备在运行安装过程中，客户对产品功能配置等方面需要的信息和需求，对业务系统影响极小。故障确诊时间：24小时，故障排除时间≤6小时。

（5）远程技术支持服务

投标人应提供7*24的服务热线，由专门受理客户问题的维护团队提供全天候不间断的产品技术咨询、故障申报受理、硬件维修受理、以及服务政策咨询等服务内容。

（6）维护性软件版本支持服务

在服务有效期内，投标人应协调原厂公司向客户提供其所购设备主机软件的维护性版本及升级版本，如：BUG修补文件，新版本的主机软件，以及该软件配套的文档资料。获得软件后，客户将享有与原有软件相同的许可权利，但不得用于商业目的的传播。

具有特殊功能并单独销售的主机软件不在提供范围内。进行License控制与销售的软件产品，如网管软件、计费软件等，只提供软件补丁，不提供新的License或新版本的软件本身。

（7）应急响应

服务类型：不定期服务

服务说明：为采购人信息系统平台提供重大安全事故和突发网络安全事件的应急响应服务。在采购人院区网络系统发生业务瘫痪、网络入侵等重大安全事故时，提供现场应急技术支持。

要求投标人30分钟内应急响应、1小时内安全技术专家到达现场处理问题、2小时内提出安全解决方案。由于硬件设备等原因不能立即解决的，提供临时解决方案建议，最大限度地保证采购人业务的正常运行。同时由投标人协调联系相关设备厂商，以保证尽快解决问题。

(8) 巡检服务

原厂可溯源技术支持工程师定期巡检服务（至少每个季度一次），对设备的运行状态进行检查和分析，提交正式服务报告。原厂可溯源技术支持工程师定期性能分析服务（至少每个季度一次），提供设备性能、高可用评估的季度分析报告，以便采购人了解维护状况，及时预见并解决问题。

(9) 重大项目现场支持

配合重大项目实施工作。根据采购人的需要，在有关项目实施中，配合完成所保设备的搬迁、系统安装调整等工作。

4、人员工作要求

投标人中标后，指定一名客户代表，制定服务计划，联系服务资源，定期与采购人技术人员交流，对维护情况进行回顾，组织和协调服务事宜，并提交阶段性服务报告。投标人技术人员按照合同要求进行服务，在现场服务时要听从采购人相关人员的安排。

5、内网准入工作

投标人所有提供服务的相关工程师及工作人员的办公电脑需配合采购人做好内网电脑入网、受控。

6、报价说明

投标人报出总价应保证其报价的充分性、完整性和符合性，以及根据自身实力所报出具有竞争力的综合取费。采购人不统一组织投标人对工程现场和其周围环境进行考察。投标人根据自身需要，确定是否自行对现场和其周围环境进行考察，以获取编制投标文件和签署实施工程所需的各项资料，及做出自己的判断和估价，并在投标时充分考虑上述因素。一旦中标后，投标人不得以不了解现场情况为由，提出任何形式的增加项目价款或索赔要求。投标人须承担现场考察的责任和风险，踏勘所发生的费用由投标人自行承担。

7、驻场人员要求

(1) 安全运维驻场服务

序号	具体要求
#1	<p>安全运维人员驻场服务（2人）：</p> <p>按采购人作息时间上下班，办公场地由采购人提供。驻场工程师通过专业技术手段落地可持续安全运营体系，围绕预测与发现、监测与分析、防御与控制、响应与管理形成的安全闭环，切实解决采购人信息安全问题。利用安全运营中心工具能够与不少于3个系统的防火墙进行联动，自动下发安全策略，以提高应急响应效率。服务内容如下：</p> <p>安全资产管理服务：</p>

- 对在网资产进行自发现和手动添加，配合安全运营中心态势监控功能，集中统一维护，对内网资产进行全方面的监测。
- 采用检查用表（checklist）定期对评估目标范围内的主机系统安全、中间件安全、数据库安全等进行系统的安全规则配置、安全策略配置、日志报警信息以及系统和软件升级、更新情况，是否存在后门等内容进行检查。

脆弱性评估服务：

- 在服务期内持续发现环境中存在的 web 应用漏洞、主机操作系统漏洞、数据库漏洞、逻辑缺陷、弱口令、信息泄露等脆弱性问题，针对扫描结果进行人工验证并去除误报，生成相关报告并提供加固建议。
- 原厂安全服务工程师对脆弱性评估结果进行人工验证，保证脆弱性评估报告的真实性。
- 提交针对性的解决方案，保证漏洞修复可落地。

日志分析服务：

- 服务工程师基于状态与行为的威胁事件检测和分析引擎，结合大数据架构集中存储的网络流量数据、安全设备和主机日志，以及外部威胁情报信息。综合多种信息元素进行全局网络的流量分析、日志分析及关联分析，深度挖掘潜在的威胁行为，还原攻击路径，发现攻击意图。
- 定期提取威胁日志数据进行安全分析，对系统遭受到的攻击方式、频率、防御有效性等方面进行数据分析总结，查找潜在的攻击痕迹，分析日志当中真实存在威胁以及病毒或木马攻击痕迹，找出确定有效的攻击，并交付日志分析报告。

风险管理服务：

- 工程师梳理终端、服务器和外网三者之间内到内、内到外、外到内之间的威胁互访关系，实现追踪攻击路径，定位攻击源，预测攻击面；
- 对安全运营中心发现的异常行为威胁事件进行提取及呈现；
- 提供所有 IOC 威胁事件分类统计和两周内威胁事件的趋势变化；
- 通过对威胁事件的分析，提炼威胁事件的核心内容及影响，使专业的威胁事件转化为简单通俗易懂的描述，便于用户分析威胁事件的影响及内

	<p>容。</p> <p>安全培训服务：</p> <p>服务要求： 驻场工程师（至少一名）具备开展信息安全意识、安全攻防技术及安全认证等方面培训的能力。要求驻场工程师具备 CISP（注册信息安全专业人员）类证书或同等能力，具有 CNVD（中国国家漏洞库）原创漏洞证明。</p> <p>服务周期：3 年。</p>
2	<p>安全事件应急服务：</p> <p>服务内容： 提供安全事件应急响应工作。在在出现重要安全事件时（信息系统遭受攻击、网络病毒爆发等），派遣高级安服人员，通过远程和现场支持的形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：突发事件相关信息的收集、事件的分析、报告提交、问题解决建议等，协助用户解决突发安全事件，并提供应急响应报告。</p> <p>服务要求： 当发生信息安全事件时，专业工程师须 10 分钟内响应并在 30 分钟内到达现场启动应急处置工作，提供安全事件处置、应急操作、安全加固建议，并协助相关部门处理安全问题；事件处置后提供事件分析处理报告，就安全风险、安全事件描述，危害性，原因、排查过程、处置加固方法进行详细说明；</p> <p>服务频率： 服务周期为 3 年，每年提供不限次数的安全应急响应服务。</p>
3	<p>安全预警通告服务：</p> <p>服务内容： 以邮件、文件、电话等方式，将安全技术和安全信息及时传递给采购人，使采购人能保持对信息安全最新动态的认识，提前预知风险，每月末以邮件方式提交安全月报。安全通告内容至少包括：目前主流操作系统的安全漏洞补丁；信息安全业界最新动态与技术；国内外最新信息安全趋势；紧急安全事件通告；最新的国内、外行业安全政策及法律法规。</p> <p>服务频率： 服务周期为 3 年，每年提供不限次数安全通告服务。</p>
4	<p>安全巡检服务：</p> <p>服务内容： 服务工程师到现场进行安全巡检服务，对客户网络及重要服务器进行分析，主要包括安全设备、系统的配置检查，对安全设备、系统的运行状态、安全策略、漏洞库等进行安全配置核查；服务器配置核查，对服务器资源、身份鉴别、默认配置、共享设置、补丁管理、日志等进行安全配置核查；安全设备日志</p>

	<p>分析，检查防火墙、入侵检测和其他安全设备的日志信息，对其进行分析，排查网络中可能发生的安全事件；服务器木马查杀，发现存在木马、病毒等恶意程序，及时进行查杀清理，避免被不法分子利用进行后续横向扩散。</p> <p>服务频率：服务周期为3年，每年提供不限次数安全加固服务。</p> <p>交付物：《安全巡检报告》</p>
5	<p>安全加固服务：</p> <p>服务内容：依据采购人的安全加固需求，对服务器、中间件、数据库、网络和安全设备提出系统加固的方案，确保系统的问题被修复或风险可控；</p> <p>服务频率：服务周期为3年，每年提供不限次数安全加固服务。</p> <p>交付物：《安全加固建议方案》</p>
6	<p>系统上线前的安全检测：</p> <p>服务内容：针对新业务系统上线前，从主机层、系统层、数据库层、中间件层全面评估新系统的安全状况，查找不符合安全要求的配置项以及安全风险点。</p> <p>服务要求：通过漏洞扫描、渗透测试、安全基线检查在内的安全评估服务手段，发现该业务系统存在安全隐患，并提出加固解决措施，协助开发单位进行整改。</p> <p>服务频率：服务周期为3年，每年提供不限次数的新系统上线检测服务。交付物：《安全风险评估报告》</p>
7	<p>设备安全策略检查优化服务：</p> <p>服务要求：服务商需定期针对采购人安全设备包括：防火墙、入侵检测系统、网闸、WAF等进行安全策略细化、调优服务。</p> <p>服务频率：服务周期为3年，每年提供不限次数设备安全策略检查优化服务。</p>

8、渗透测试服务

技术项	具体要求
服务概述	<p>渗透测试是为了证明采购人互联网服务的网络防御按照预期计划正常运行而提供的一种机制，由安全专家模拟恶意黑客的攻击行为，通过远程方式对信息系统进行非破坏性的入侵测试。</p> <p>这个过程包括对系统的任何弱点、技术缺陷或漏洞的主动分析。渗透测试可以发现逻辑性更强、更深层次的漏洞，并直观反映漏洞的潜在危害，更加真</p>

	<p>实的了解到信息系统的安全性状况，为信息系统的安全配置与管理提供指导建议。</p>
<p>服务内容</p>	<p>1、针对 Windows、Linux、SCO 和 SGI 等操作系统，进行漏洞识别和分析。这些漏洞通常分为远程漏洞利用执行和本地漏洞利用执行，需结合实际环境进行系统性评估，及时修补安全隐患，防止攻击者利用漏洞进行恶意活动。</p> <p>2、识别由 ASP、CGI、JSP 和 PHP 等技术构建的 Web 应用程序（约 25 个应用程序）中的安全漏洞。常见的漏洞包括 SQL 注入、跨站脚本（XSS）、文件上传漏洞、文件解析错误、配置不当、目录遍历、命令执行及文件包含等。路由器、防火墙、交换机等网络设备在网络传输中扮演着关键角色，安全性至关重要。通过识别这些设备中的拒绝服务漏洞和绕过（bypass）漏洞，全面评估网络基础设施的安全状况，确保网络通信的稳定与安全。</p> <p>3、应用层的渗透测试应至少支持以下安全漏洞的检测，涵盖但不限于：网站结构分析、目录遍历探测、隐藏文件探测、备份文件探测、CGI 漏洞扫描、用户名与密码猜解、跨站脚本漏洞挖掘、SQL 注入漏洞挖掘及数据库挖掘分析。通过全面的测试，能够及时发现潜在安全风险，并为后续的安全加固提供依据。</p> <p>4、测试过程中需遵循最小影响原则，避免对生产环境造成业务中断或数据损坏；所有操作须经授权并记录完整审计日志，确保可追溯、可复核。同时，应结合人工验证与自动化工具，提升漏洞识别准确率，降低误报漏报风险。</p>
<p>服务流程</p>	<p>1、前期准备阶段</p> <p>在实施渗透测试工作前，技术人员和用户对渗透测试服务相关的技术细节进行详细沟通。由此确认渗透测试的方案，方案内容主要包括确认的渗透测试范围、最终对象、测试方式、测试要求的时间等内容。</p> <p>2、测试阶段实施</p> <p>测试人员首先使用自动化的安全扫描工具，完成初步的信息收集、服务判断、版本判断、补丁判断等工作。然后由人工的方式对安全扫描的结果进行人工的确认和分析。并且根据收集的各类信息进行人工的进一步渗透测试深入。</p> <p>结合自动化测试和人工测试两方的结果，测试人员需整理渗透测试服务的输出结果并编制渗透测试报告，并基于漏洞的严重程度、加固措施实施的难易</p>

	<p>程度、降低风险的时间紧迫性，以及所需的人力和资金成本等多种因素，提出切实可行的漏洞整改建议，最终提交用户和对报告内容进行沟通。</p> <p>3、复测阶段实施</p> <p>在经过第一次渗透测试报告提交和沟通后，等待用户针对渗透测试发现的问题整改或加固。经整改或加固后，测试人员进行回归测试，即二次复测。复测结束后提交给用户复测报告和对复测结果进行沟通。</p> <p>4、成果汇报阶段</p> <p>根据一次渗透测试和二次复测结果，整理渗透测试服务输出成果，最后进行成果汇报。</p>
服务频率	★ 服务周期为3年，每年开展两次全面渗透测试，单次渗透测试的范围至少包含20个业务系统。
交付物	《渗透测试报告》、《渗透测试复测报告》
服务要求	# 渗透测试服务工程师应熟悉和掌握不同的渗透测试工具和技术，拥有强大的漏洞挖掘与分析能力，具备安全评估与报告撰写能力，应具备注册信息安全人员渗透测试专家（CISP-PTE）证书。

9、维保服务清单

序号	维保设备/系统名称	维保设备品牌、型号	维保内容	数量
1	态势感知平台	山石 SG-6000-1SC6220	设备维保及特征库升级	1
2	威胁感知设备	山石 BDS-12830	设备维保及特征库升级	1
3	威胁感知设备	山石 BDS-12850	设备维保及特征库升级	1
4	WAF（WEB应用防火墙）	长亭 SL-H20-HG-3000	设备维保及特征库升级	1
5	外网出口防火墙-主	山石 SG-6000-K5680	设备维保及特征库升级	1
6	外网出口防火墙-备	山石 SG-6000-K5680	设备维保及特征库升级	1
7	外网出口IPS-主	山石 SG6000-S2580-GC	设备维保及特征库升级	1
8	外网出口IPS-备	山石 SG6000-S2580-GC	设备维保及特征库升级	1
9	新数据中心防火墙-主	山石 SG-6000-K5680	设备维保及特征库升级	1
10	新数据中心防火墙-备	山石 SG-6000-K5680	设备维保及特征库升级	1

11	网闸防火墙	山石 SG-6000-E2868	设备维保及特征库升级	1
12	漏洞扫描	绿盟 NX3	设备维保及特征库升级	1

包 4：网络系统维保服务要求

1、维护的要求和期限

(1) 提供软、硬件基本维保服务，包括但不限于提供网络设备、网管系统技术现场服务，硬件备件更换现场服务，软、硬件版本升级现场服务，核心设备故障排错及恢复业务服务等，确保能迅速解决采购人核心业务网设备故障、排除运行隐患，保证采购人各项业务的稳定运行。为确保设备兼容性与技术支持连续性，投标人需提供原厂可溯源的维保服务。如提供非原厂服务，须提供原厂授权证明及同等质量的技术保障承诺，经采购人书面确认后方可实施。

(2) 维护期限：自合同签订之日起3年。

2、维护工作范围

★(1) 投标人为采购人网络、安全设备及网管系统提供 3 年产品原厂可溯源维保服务；服务标准为 7*24 小时级别，参保设备维护期限为 3 年，自合同签订之日起。

#(2) 中标后投标人应提供维保清单内具有满足本项目采购需求的售后服务证明文件，包括但不限于售后服务承诺函或授权函等。

(3) 负责本次招标所有系统设备的技术支持和运行维护工作。

3、维护工作内容和标准

总体描述：客户服务经理与支持团队、快速备件更换、现场技术支持、维护性软件版本支持以及网站支持等内容。能够有效帮助采购人技术支持人员维护网络稳定运行，满足采购人对高效、稳定的网络环境的需求。

(1) 网络设备、网管系统参保须为原厂可溯源保修：中标人需确保采购人所要求维保服务清单内软、硬件设备故障保修为原厂可溯源保修或备件更换。

(2) 客户服务经理与支持团队：在设备维保期内，投标人须指定专责服务主管、专责工程师团队、专职项目经理，项目经理的更换须得到采购人同意。

★(3) 快速备件先行更换服务：投标人应向采购人提供及时周到的原厂可溯源快速备件更换服务。服务标准为备件先行7*24响应。

一旦定位是硬件故障，中标人应在规定时间内将原厂可溯源正品备件先行运抵现场，保证故障部件得到及时更换，以使采购人的业务能在最短时间内恢复正常。

#(4) 工程师快速现场支持服务：考虑到采购人信息系统组网复杂，业务重要，且设备均为高端产品，在业务出现问题或者设备出现问题时，需要及时排查并能迅速解决，故此，投标人应承诺在重大法定节假日、重大接入网故障事件，重要切换、上线、变更、切换演练等大型网络变动时提供现场技术支持服务。具体内容包括但不限于：

A. 工程师快速现场支持到达现场支持；

B. 现场备件更换支持服务；

C. 现场故障诊断及故障排除;

D. 现场软件升级。

投标人工程师及投标人安排的原厂可溯源技术支持工程师，自接到首次现场支持通知（电话、短信、微信等）时起，到达指定现场的时间要求为1小时内。首次通知无响应的（包括但不限于电话不接或挂断、短信不回复、微信不回复等，以采购人定义为准），均视为通知已到达并开始计算时限，如不能按时（1小时内）抵达现场，每次处以2000元人民币罚款。一年服务期内，累计超过3次不能按时抵达现场的情况，采购人有权终止合作及合同履行，并终止支付合同款项且不承担任何相关责任。

技术支持具体响应时间定义如下：

P1级故障——设备在运行故障中出现整机系统瘫痪或服务中断，导致设备的基本功能不能实现或全面退化的故障。故障确诊时间:1小时，故障排除时间≤8小时。

P2级故障——设备在运行中出现的故障具有潜在的系统瘫痪或服务中断的危险，并可能导致设备的基本功能不能实现或全面退化。故障确诊时间：3小时，故障排除时间≤6小时。

P3级故障——设备在运行中出现影响业务，并导致系统性能或服务部分退化的故障。故障确诊时间：12小时，故障排除时间≤6小时。

P4级故障——咨询类问题或设备在运行安装过程中，客户对产品功能配置等方面需要的信息和需求，对业务系统影响极小。故障确诊时间：24小时，故障排除时间≤6小时。

（5）远程技术支持服务

投标人应提供7*24的服务热线，由专门受理客户问题的维护团提供全天候不间断的产品技术咨询、故障申报受理、硬件维修受理、以及服务政策咨询等服务内容。

（6）维护性软件版本支持服务

在服务有效期内，投标人应协调原厂公司向客户提供其所购设备的主机软件的维护性版本及升级版本，如：BUG修补文件，新版本的主机软件，以及该软件配套的文档资料。获得软件后，客户将享有与原有软件相同的许可权利，但不得用于商业目的的传播。

具有特殊功能并单独销售的主机软件不在提供范围内。进行License控制与销售的软件产品，如网管软件、计费软件等，只提供软件补丁，不提供新的License或新版本的软件本身。

（7）应急响应

服务类型：不定期服务

服务说明：为采购人信息系统平台提供重大安全事故和突发网络安全事件的应急响应服务。在采购人院区网络系统发生业务瘫痪、网络入侵等重大安全事故时，提供现场应急技术支持。

要求投标人30分钟内应急响应、1小时内安全技术专家到达现场处理问题、2小时内提出安全解决方案。由于硬件设备等原因不能立即解决的，提供临时解决方案建议，最大限度地

保证采购人业务的正常运行。同时由投标人协调联系相关设备厂商，以保证尽快解决问题。

(8) 巡检服务

原厂可溯源技术支持工程师定期巡检服务（至少每个季度一次），对设备的运行状态进行检查和分析，提交正式服务报告。原厂可溯源技术支持工程师定期性能分析服务（至少每个季度一次），提供设备性能、高可用评估的季度分析报告，以便采购人了解维护状况，及时预见并解决问题。

(9) 重大项目现场支持

配合重大项目实施工作。根据采购人的需要，在有关项目实施中，配合完成所保设备的搬迁、系统安装调整等工作。

4、人员工作要求

投标人中标后，指定一名客户代表，制定服务计划，联系服务资源，定期与采购人技术人员交流，对维护情况进行回顾，组织和协调服务事宜，并提交阶段性服务报告。投标人技术人员按照合同要求进行服务，在现场服务时要听从采购人相关人员的安排。

5、内网准入工作

投标人所有提供服务的相关工程师及工作人员的办公电脑需配合采购人做好内网电脑入网、受控。

6、报价说明

投标人报出总价应保证其报价的充分性、完整性和符合性，以及根据自身实力所报出具有竞争力的综合取费。采购人不统一组织投标人对工程现场和其周围环境进行考察。投标人根据自身需要，确定是否自行对现场和其周围环境进行考察，以获取编制投标文件和签署实施工程所需的各项资料，及做出自己的判断和估价，并在投标时充分考虑上述因素。一旦中标后，投标人不得以不了解现场情况为由，提出任何形式的增加项目价款或索赔要求。投标人须承担现场考察的责任和风险，踏勘所发生的费用由投标人自行承担。

7、驻场人员要求

(1) 网络运维驻场服务

序号	具体要求
1	<p>网络运维人员驻场服务（1人）：</p> <p>（1）服务期内，投标人需要提供1名网络工程师进行驻场服务。驻场工程师要求有三年以上网络设备运维工作经验，具备厂商中级及以上认证证书（或具有同等能力水平）。具体工作包括以下内容：</p> <p>A. 日常设备维护。精通常见网络设备（如：新华三、华为等）日常运维、巡检、故障定位与处置能力，精通网管软件日常运维、巡检、故障定位与处置能力，</p>

	<p>具备本次招标涉及的设备及系统的日常运维能力，必要时能够进行调整和优化，保障平台正常运行；</p> <p>B. 补丁、版本升级服务。及时对采购人网络设备及网管软件进行软件补丁、版本升级，使数据中心各项设备处于良好运行状态；</p> <p>C. 故障处理。预警并协助数据中心预防重大故障的发生，在发生故障时可以快速解决故障；</p> <p>D. 保障服务。为了保障重大节日期间机房软硬件支撑环境安全运行，向我方提供现场工程师值守服务，并在保障结束后提供服务总结报告和建议；</p> <p>E. 其他现场技术支持服务。包括相关技术咨询、新需求的配合解决、配合割接实施等其他现场技术支持服务；</p> <p>F. 考勤要求。驻场工程师按采购人作息时间上下班，办公场地由采购人提供。</p>
--	---

8、维保服务清单

序号	设备型号	设备类型	产品描述	数量
1	核心交换机 S12508X	LSWM1QSTK2	功能模块-H3C S5820V2-LSWM1QSTK2-40G QSFP+电缆-5m-国内海外合一版	4
		PSR2400-54A	功能模块-H3C S12500X-AF-LSXM1PSRA-2400W 交流电源模块-国内海外合一版	8
		LSXM1SUPB1	功能模块-H3C S12500X-AF-LSXM1SUPB1-主控制引擎模块-国内海外合一版	4
		LSXM108XFAN	功能模块-H3C S12508X-AF-LSXM108XFAN-以太网交换机风扇模块-国内海外合一版	4
		LSXM1IMA	功能模块-H3C S12500X-AF-LSXM1IMA-业务板适配器-国内版	4
		LSXM1GT48FX1	功能模块-H3C S12500-X-LSXM1GT48FX1-48 端口千兆以太网电接口模块 (RJ45) (FX)-国内版	2
		LSXM1TGS24FX1	功能模块-H3C S12500-X-LSXM1TGS24FX1-24 端口万兆以太网光接口模块 (SFP+, LC) (FX)-国内版	2
		LSXM1SFF08A1	功能模块-H3C	12

			S12508X-AF-LSXM1SFF08A1-交换网板-F型(A类)-国内版	
		LS-12508X-AF	装配组件-H3C S12508X-AF-LSXZ108X-以太网交换机主机-国内海外合一版	2
2	核心交换机 S10506	LSUM1MPU06B0	功能模块-H3C S10506-LSUM1MPU06B0-主控交换模块-国内版	2
		LSUM1FAB06C0	功能模块-H3C S10506-LSUM1FAB06C0-交换网板-C类-国内版	1
		LSUM2GT24PTSSE0	功能模块-H3C S10500-LSUM2GT24PTSSE0-24端口千兆以太网电接口(RJ45)+20端口千兆以太网光接口(SFP, LC)+4端口万兆以太网光接口模块(SFP+, LC)(SE)-国内海外合一版	1
		LSUM1TGS16FD0	功能模块-H3C S10500-LSUM1TGS16FD0-16端口万兆以太网光接口模块(SFP+, LC)(FD)-国内海外合一版	1
		LS-10506	装配组件-H3C S10506-LSUZ110506-以太网交换机主机-国内版	1
		LSUM1AC2500	功能模块-H3C S10500-LSUM1AC2500-2500W交流电源模块-国内海外合一版	2
3	无线控制器	EWP-WX3520H	H3C WX3520H 无线控制器	1
		LSPM2150A	150W 资产管理交流电源模块	2
4	流控与上网行为审计 ACG1000	NS-SecPath ACG1000-X	数据通信-H3C SecPath ACG1000-X-应用控制网关主机(4GE Combo+3Slots)-国内版	1
		AC-PSR300-12A2	功能模块-H3C MSR-RTUM1PWR300A-300W AC电源模块-国内版	2
		NSQM1TGS4	数据通信-H3C SecPath ACG1000-E-4端口万兆以太网模块(SFP+)接口卡-国内版	1
5	核心交换机 S10510	LS-10510	装配组件-H3C S10510-LSUZ110510-以太网交换机主机-国内版	2
		LSUM1TGS24FD0	功能模块-H3C S10500-LSUM1TGS24FD0-24	3

			端口万兆以太网光接口模块 (SFP+, LC) (FD)-国内海外合一版	
		LSUM1FAB10C0	功能模块-H3C S10510-LSUM1FAB10C0-交换网板-C类-国内版	4
		LSUM1MPU10C0	功能模块-H3C S10510-LSUM1MPU10C0-主控交换模块-国内版	4
		LSUM1AC2500	功能模块-H3C S10500-LSUM1AC2500-2500W 交流电源模块-国内海外合一版	4
6	无线控制器 WX5540H	EWP-WX5540H	装配组件-H3C WX5540H-EWPXZ15540H-无线控制器主机(12GE+12SFP+4SFP Plus)-国内海外合一版	2
		LSPM2150A	150W 资产管理交流电源模块	4
7	核心交换机 7506E	LS-7506E-NonPoE	装配组件-H3C S7506E-LSQZ17506ENP-以太网交换机主机-非 PoE-国内版	1
		LSQM3MPUB0	功能模块-H3C S7506E-NonPoE-LSQM3MPUB0-主控交换模块-国内海外合一版	2
		LSQM1AC650C	以太网交换机交流电源模块-650W	2
		LSQM2GT24PTSSC0	功能模块-H3C S7500E-LSQM2GT24PTSSC0-24 端口千兆以太网电接口 (RJ45)+20 端口千兆以太网光接口 (SFP, LC) +4 端口万兆以太网光接口模块 (SFP+, LC) (SC)-国内海外合一版	1
8	网管系统	SWP-IMC7-IMP	H3C iMC-智能管理平台标准版, 医院内网和外网各一套, 外网包含 EIA 准入模块	2 套
9	接入交换机	LS-5130S-28P-HPWR-EI	数据通信-H3C S5130S-28P-HPWR-EI-LS5Z1S28PHPE-L2 以太网交换机主机 (24GE (PoE+) +4SFP+4GE Combo) - (AC/DC) -国内版	38

包 5：弱电智能化维保服务要求

1、维护工作范围

1.1 弱电智能化系统运维服务清单如下：

序号	弱电智能化子系统名称	现有品牌	范围	运维服务期	
1	监控系统	海康威视	全院区	3 年	
2	门禁系统	新开普/道尔	全院区	3 年	
3	其他弱电智能化系统	综合布线系统	康普	全院区	3 年
4		时钟系统	斯泰科	全院区	3 年
5		电子巡更系统	兰德华	全院区	3 年
6		一键报警系统	玛斯康	全院区	3 年
7		多媒体会议系统	华为/宝利通	全院区	3 年
8		电梯无线对讲系统	海康威视/大华	全院区	3 年

1.2 维护要求：

1.2.1 监控系统技术支持服务：提供监控系统 3 年技术支持服务，每年不少于 5 次现场支持服务和不少于 4 次远程技术支持服务，为确保设备兼容性与技术支持连续性，投标人需提供原厂可溯源的维保服务。如提供非原厂服务，须提供原厂授权证明及同等质量的技术保障承诺，经采购人书面确认后方可实施。

#1.2.2 门禁系统技术支持服务：提供门禁系统 3 年技术支持服务，每年不少于 5 次现场支持服务和不少于 4 次远程技术支持服务，为确保设备兼容性与技术支持连续性，投标人需提供原厂可溯源的维保服务。如提供非原厂服务，须提供原厂授权证明及同等质量的技术保障承诺，经采购人书面确认后方可实施。

1.2.3 提供弱电智能化系统运维服务清单内所有设备的 3 年技术运维服务。

2、服务期限

维护期限：自合同签订之日起 3 年。

3、服务要求及内容

3.1 运维人员服务内容

★要求按照弱电智能化系统运维的要求，提供专业的人员进行驻场服务，提供不少于 3 名现场驻场运维工程师。

运维服务内容：

(1) 监控系统运维服务:至少提供固定驻场人员 1 名, 包含全院监控系统安装、维修、调试与软件服务, 运维服务期限: 3 年。

(2) 门禁系统运维服务:至少提供固定驻场人员 1 名, 包含全院门禁系统安装、维修、调试与软件服务, 运维服务期限: 3 年。

(3) 其他运维系统服务:至少提供固定驻场人员 1 名, 包含综合布线、时钟系统、电子巡更、一键报警、多媒体会议、电梯无线对讲等系统运维服务, 运维服务期限: 3 年。

3.2 运维服务人员要求

(1) 投标人需指定 1 名项目经理作为此项目的主要负责人(项目经理)。项目经理的职责包括但不限于以下内容:

①负责制定维护方案和协调资源以满足采购人弱电系统运维项目的工作需求。

②负责制定维护服务计划, 包括例行的技术巡检。

③负责应对突发事件的应急响应和人员组织以及事后报告。

④负责配合采购人在关键时间节点期间做好应急保障工作。

(2) 项目经理应满足以下要求:

①项目经理须具备本科及以上学历、同时具备信息系统项目管理师高级证书, 提供证书及 2025 年 6 月以来不少于 3 个月的本公司社会保险缴纳证明材料。

②应全面掌握弱电智能化系统运维相关知识及本次招标运维服务清单中各系统的专业知识, 并具有相应工作经验。

③项目经理应了解弱电智能化系统的各类基础系统的基本信息及运行工况, 能够统筹协调处理疑难问题, 或提供解决方案。

④项目经理应做好 24 小时的应急响应, 处理紧急事件时确保 1 小时内到达。

(3) 驻场运维服务团队工程师的要求:

①驻场运维服务团队中工程师至少有 1 人同时具备系统集成项目管理工程师证书和一级建造师执业资格证书(通信与广电工程专业), 提供证书及 2025 年 6 月以来不少于 3 个月的本公司社会保险缴纳证明材料。

②驻场运维服务团队中工程师至少有 2 人具备人社部门颁发的通信专业技术人员职业资格证书(终端与业务专业), 提供证书及 2025 年 6 月以来不少于 3 个月的的本公司社会保险缴纳证明材料。

③要求驻场运维团队工程师具备至少 5 年以上工作经验, 以毕业时间为准, 提供毕业证书复印件。

④要求驻场运维团队工程师具备弱电运维实操技术能力，中标人提供驻场人员时，需进行评估验证，包含但不限于：工具熟练使用、问题定位排查、硬件维修能力、链路修复能力等。

3.3 服务内容要求：

3.3.1 系统或硬件故障排除

系统或硬件出现故障时，维保工程师到达现场，检测故障原因，若非设备故障，应及时排除。

3.3.2 巡检服务

每月进行一次巡检服务，对设备进行现场硬件设备和线路巡检，包括各个配件的检测、链接状态、整机运行状态检测，并提供巡检报告。

3.3.3 运维响应

技术人员 7*24 小时电话支持和现场支持，获得与硬件问题相关的技术咨询或故障排除帮助。对于非硬件故障，1 小时内积极协助解决问题。对于硬件故障，要求 12 小时内故障备件到达现场，若非设备故障，24 小时内完成维修服务。

4、项目技术支持服务要求

项目技术支持服务要求包括故障修复要求、技术咨询要求、专业设备要求、维保团队的要求、维护人员要求、备件库要求和其他要求。

4.1 故障修复要求

(1) 投标人须定期对运维服务系统进行全面技术检查、维护及保养，并做详细检查记录，记录包含巡检单维修单年度维护报告。

(2) 在整个维护服务保修期内，投标人应提供 7*24 的故障修复服务。对当日无法解决的故障或故障设备将影响系统正常运行的，应提供代用设备或应急解决方案，并确保系统正常运行。故障排除后，投标人须出具故障处理报告，帮助采购人进行故障根源的分析和诊断，提出后续工作的改进措施。

4.2 技术咨询要求

(1) 投标人应免费提供技术咨询服务，包括新产品新技术通报，软硬件技术咨询，系统改进意见，提供技术解决方案(如:重要割接操作事前方案等)，项目长远规划，研究解决技术难题。

(2) 投标人须以书面形式告知采购人 7*24 小时的专用维保不限于服务电话、移动电话、电子邮件、传真等联系方式以及提供支持服务过程中需要采购人准备的设备信息(如产品序

列号等), 用于受理故障报修, 解答采购人的技术咨询问题。如联系方式有变动, 投标人须提前以书面形式通知采购人。

4.3 专业设备要求

投标人应具有专业仪器仪表以及专业维修工具。

包含但不限于: 工具包、万用表、寻线仪、压线钳、打线枪、剥线钳、螺丝刀、电笔、头灯、胶枪、冲击钻、标签打印机、人字梯、板车等以及其他弱电系统常用维修配件。

4.4 运维团队要求

投标人应具有专业的运维服务工程师团队, 可对提供运维的弱电子系统设施进行完整维护及必要的健康年度检查, 并提供专业方案。

5、运维服务具体要求如下:

序号	运维系统	运维服务要求
1	监控系统	<p>1. 前端系统日常运行维护服务: 包括摄像头的日常维护、故障排查和修复等。</p> <p>2. 后端平台运行维护及统筹调度服务: 包括平台软件及服务端的更新、维护以及调度系统的优化等。</p> <p>3. 网络链路运行维护服务: 确保视频数据传输的稳定性。</p> <p>4. 易损件与备品备件管理服务: 确保系统各部件的及时更换和维护。</p> <p>5. 至少提供固定驻场人员 1 名, 包含 10 个点位/年的新装服务 (包含硬件及线材), 以及监控系统安装、维修、调试与软件服务。</p>
2	门禁系统	<p>1. 前端设备</p> <p>①读卡器: 对读卡器刷卡的灵敏度进行测试。</p> <p>②可视呼叫: 对可视呼叫设备进行测试。</p> <p>③人脸识别: 对人脸识别设备进行测试。</p> <p>④单元保护器: 单元保护器对读卡器、电磁锁之间的电源电压是否正常。</p> <p>⑤联网控制器: 联网功能正常调节, 测试与服务器通讯是否正常。</p> <p>⑥门磁、门吸: 是否能够正常关闭, 正常吸合。</p> <p>2. 传输系统</p> <p>①信号传输线路: 线路连接状态, 信号传输衰减, 绝缘电阻大小, 有无线路干扰, 有无氧化。</p> <p>3. 监控中心</p>

		<p>①中心主机：联网通信测试，保障通信正常。</p> <p>②通信器：工作状态是否正常。</p> <p>4. 包括门禁系统的维护和保养工作，确保系统及服务端的安全、可靠运行。具体服务范围可能包括设备检查、维修、保养、软件更新、故障排除等。</p> <p>5. 至少提供固定驻场人员 1 名, 包含 10 个点位/年的新装服务(包含硬件及线材)，以及门禁系统维修、调试与软件服务。</p>
3	其它智能化系统	<p>1. 综合布线系统</p> <p>①清除机柜内外综合布线系统上的灰尘。</p> <p>②检查综合布线桥架的平整度，如果发生变形、支架螺丝脱落等与安装图纸不相符合的情况应立即修复。以免桥架断裂或脱落致使信息业务突然中断。</p> <p>③检查双绞线上、面板上、配线架、跳线上的标签，将脱落的标签补全，将粘连不牢的标签固定好，更换有损伤的标签。</p> <p>④使用性能测试仪对铜缆信道和未使用的光纤信道进行抽检，测试方法为永久链路测试和所用跳线的性能测试，并与原始记录进行核对。</p> <p>⑤维护与保养：对弱电线路、模块出现的故障、损坏，进行问题定位，并及时维修或更换。</p> <p>⑥包含 200 个点位/年的信息点位的综合布线施工服务（包含硬件及线材）</p> <p>2. 时钟系统</p> <p>①母钟主机运维：核心母钟 / 授时主机运行稳定，GPS / 北斗授时模块工作正常，无死机、程序故障，时间基准精准。</p> <p>②子钟终端巡检：各类数字 / 指针子钟显示清晰、走时准确，无黑屏、跳字、卡滞，按键 / 调光功能正常，安装牢固。</p> <p>③授时链路保障：GPS / 北斗天线、网络授时链路、同步信号线无松动遮挡，信号强度达标，授时无断连延迟。</p> <p>④时间同步核验：定期核对子母钟时间一致性，偏差≤规范值，联动弱电其他系统（安防 / 会议 / 报警）时钟同步生效。</p> <p>⑤电源及备用保障：主供电、UPS 后备电源巡检，供电稳定无断电，子钟断电续航正常，防雷防浪涌有效。</p> <p>⑥故障处置及校准：快速排查走时偏差、授时失效、显示故障，定期校准时间精度，留存巡检校准台账。</p>

		<p>3. 电子巡更系统</p> <p>①巡更终端运维：巡检巡更棒 / 手机终端，确保开机正常、读卡灵敏、电量充足，无磕碰故障。</p> <p>②巡更点位保障：检查现场巡更点 / 信息钮，无松动脱落、损坏遮挡，安装牢固且感应正常。</p> <p>③数据传输核验：确保巡更数据无线 / 有线上传后台无丢失、延迟，读卡记录实时同步。</p> <p>④软件系统维护：后台巡更管理软件运行稳定，排班、数据查询 / 统计 / 导出正常，权限合规。</p> <p>⑤电源及配件管理：巡更终端充电、备用电池 / 充电器完好，充电正常，配件无缺失损坏。</p> <p>⑥台账及故障处置：核对巡更记录完整性，快速排查读卡、传输、软件故障，留存运维台账。</p> <hr/> <p>4. 一键报警系统</p> <p>①前端设备巡检：一键报警按钮、紧急呼叫终端、声光报警器的外观完好、按键灵敏、供电正常，无损坏 / 松动 / 故障。</p> <p>②通讯链路保障：检查网线、4G/5G、无线网桥等传输链路，确保报警信号实时上传，无断连、延迟、丢包问题。</p> <p>③平台系统维护：后台主机 / 服务器运行稳定，软件无卡顿 / 闪退，权限管理合规，报警信息存储 / 查询正常，及时更新系统补丁。</p> <p>④报警联动测试：定期模拟一键报警，验证平台接收、声光提示、联动监控 / 对讲 / 安防主机等功能是否生效，确保报警闭环。</p> <p>⑤电源及备用保障：主电源、UPS 不间断电源、后备电池巡检，保证断电时设备正常工作，电池续航达标。</p> <p>⑥故障处置及台账：快速排查设备 / 信号 / 联动故障并修复，记录巡检、测试、故障处理台账，留存运维记录。</p> <hr/> <p>5. 多媒体会议系统</p> <p>①音视频设备巡检：麦克风、音箱、摄像头、投影仪 / 大屏、拾音器，确保拾音 / 发声清晰、画面无卡顿偏色、镜头转动对焦正常。</p> <p>②终端设备保障：会议主机、中控系统、投屏终端、调音台 / 功放，运行稳定无死机，按键/触控操作灵敏，接口无松动损坏。</p> <p>③传输链路维护：HDMI/光纤/网线、无线投屏/蓝牙链路，信号</p>
--	--	--

		<p>无断连/花屏/延迟，投屏、音视频同步传输正常。</p> <p>④软件系统运维：会议软件、中控程序、投屏软件，版本适配无闪退，权限配置合规，会议记录/投屏功能正常。</p> <p>⑤电源时序管理：时序电源、UPS 备用电源，供电稳定无跳闸，设备开关机顺序合规，断电应急供电有效。</p> <p>⑥会前调试 + 故障处置：会前提前全功能测试，快速排查音画、投屏、连接故障，保障会议全程顺畅，留存运维记录。</p> <p>6. 电梯无线对讲系统</p> <p>①无线链路巡检：机房 / 轿厢无线网桥、天线、模块，确保井道 / 轿厢信号稳定无断连、强度达标，漫游切换顺畅无卡顿。</p> <p>②对接设备保障：无线网关、电梯对讲分机 / 主机、数据采集终端，运行无死机，接口无松动，对讲通话清晰无杂音。</p> <p>③信号联动核验：验证电梯呼叫、楼层状态、困人报警等信号，无线上传后台精准无延迟，对接功能闭环生效。</p> <p>④电源及防雷运维：设备供电、UPS 后备电源、防雷模块巡检，供电稳定，防雷防浪涌，断电应急通讯正常。</p> <p>⑤故障处置及台账：快速排查信号、对接、联动故障，记录巡检 / 测试 / 维修台账，同步电梯设备运行状态。</p> <p>7. 以上运维子系统至少提供固定驻场人员 1 名，包含综合布线、时钟系统、电子巡更、一键报警、多媒体会议系统、电梯无线对讲等系统及服务。</p>
4	备品备件及其他服务	<p>1. 监控系统常见备件和易损件，以及免费更换服务。</p> <p>2. 门禁系统常见备件和易损件，以及免费更换服务。</p> <p>3. 综合布线系统常见备件和易损件，以及免费更换服务。</p> <p>4. 其它智能化系统常见备件和易损件，以及免费更换服务。</p>

6、运维人员管理要求：

(1) 运维工程师在提供服务期间需接受采购人管理，服从医院工作安排，严格遵守采购人的各项管理及规章制度。采购人信息中心对运维工程师进行管理、考核、监督及评价。人员调整、更换、离职、变动等，需至少提前 1 个月向医院信息中心提出申请，也需要经过信息中心负责人书面签字确认后方可进行，如中标人未经信息中心确认进行人员调整，医院有权终止合同并提出赔偿。一自然年内大于 2 人次主动申请更换人员，自第 3 人次起，每次将从履约保证金中扣罚 5000 元。

(2) 如人员无法满足现场工作要求，信息中心将书面通知中标人更换人员，中标人在收到信息中心书面通知 15 日内，需要将人员调整更换到位（通知会以邮件或者信函方式给到中标人，中标人需在合同签订时，主动提供联系电子邮箱及通讯地址）。一自然年内大于 2 人次书面通知中标人更换人员，自第 3 人次起，每次将从履约保证金中扣罚 5000 元。

关于“人次”，举例说明：1 次申请或通知更换 1 人，为 1 人次；一次申请或通知更换 3 人，为 3 人次。

(3) 服务期内，双方须签订保密协议，供应商须严格保护采购人系统、数据、信息的安全，不得泄露服务过程中获取的敏感信息。由于供应商违反保密协议而导致的泄密或给采购人造成损失的，由供应商负全责，并由供应商赔偿采购人所有损失；构成犯罪的，移交司法机关处理。

(4) 事件管理：当涉及下述情况当中的任何一种时，即视为紧急事件。对于紧急事件，需要按照最高优先级立即进行处理，并在接到反馈问题后立即上报信息中心。

- A、医院院领导直接指示或者由其他人员转达院领导所通知的需处理问题。
- B、大型检查、视察、考核、参观、创先活动期间，涉及区域的维护问题。
- C、地震、火灾、停电、漏水、断网、网络设备宕机等原因所造成的大面积故障。
- D、医院总值班反馈的问题以及所有因对沟通或服务不满所产生的投诉事件。
- E、影响医院或科室正常工作秩序的紧急问题。
- F、其他临时交办事宜。

★7、服务方式：（要求投标人提供加盖公章的承诺函）

- (1) 提供 7*24 小时服务，随时电话畅通。
- (2) 提供现场驻场服务，按采购人作息时间上下班，办公场地由采购人提供。工作时间以医院实际工作安排为准，非工作时间，需到现场处理的，要求响应时间不得超过 30 分钟。周末和节假日需安排人员值班，确保全年度 7*24 小时有人在岗。
- (3) 提供应急保障服务，在重大任务期间或关键时间，要求提供 7*24 小时不间断现场值守服务。
- (4) 提供原厂可溯源技术支持服务，能够随时指导、协助驻场人员处理问题，必要时能够上门服务。

8、响应要求：

- (1) 接到服务需求后，驻场人员 30 分钟内到达现场，2 小时内处理完成。
- (2) 驻场人员无法解决故障时，原厂可溯源技术工程师须在 2 小时内到达现场，并立

即开始不间断现场支持。

不同级别故障，分别承诺不同的解决时限。

故障级别	故障描述	解决时限
一级故障	系统瘫痪、设备无法运行或网络中断，影响生产经营活动正常运行的故障。	2 小时
二级故障	现有设备的操作性能严重下降，或由于设备性能明显下降，使最终的业务运作重要影响。	6 小时
三级故障	设备的操作性能受损，但大部分业务运作仍可正常工作	12 小时
四级故障	在产品功能安装或配置方面需要信息或支援，对业务系统影响极小	24 小时