目录

❶、信息安全服务要求 2

（一）安全托管服务要求 2

（二）渗透测试服务要求 6

（三）红队检测（攻防演练） 7

❷、IT核心机房运维技术要求 8

（一）、IT核心机房运维设备情况 8

（二）、IT核心机房运维服务要求 8

（三）、IT核心机房运维需续保设备清单 10

1、 安全设备三年过保后硬件维保购置及软件升级购置（2024年5月过保） 10

2、 云管理平台软件原厂软件升级更新续保（ZStack Cloud）（2023年9月过保） 11

3、 虚拟化存储软件三年过保后维保购置原厂软件升级续保（xsky）（2023年1月过保） 11

4、 云平台计算资源服务器6+1台（曙光H620-G30）三年过保续保购置原厂核心部件更换 11

5、 存储系统计算节点3台（曙光H620-G30）三年过保续保购置原厂核心部件更换 11

❸信息化硬件终端运维服务 12

（一）维护保养及维修服务范围 12

（二）人员配置及维修维护要求 13

（三）维护维修服务工作具体要求 13

一、维护内容： 13

二、日常监控： 14

三、预防性维护与巡检： 14

四、版本升级与增强： 14

五、设备维修： 14

# ❶、信息安全服务要求

我院现有安全设备清单

|  |  |  |
| --- | --- | --- |
| **序号** | **型号** | **数量** |
| 1 | AF-1000-B1800 | 2 |
| 2 | DAS-1000-A620S | 1 |
| 3 | AC-1000-B1400 | 1 |
| 4 | AF-1000-B1400 | 2 |
| 5 | OSM-1000-B1150 | 1 |
| 6 | STA-100-B2100 | 1 |
| 7 | SIP-1000-F600 | 1 |
| 8 | LAS-1000-C600 | 1 |
| 9 | BVT-1000-B1150 | 1 |
| 10 | EDR | 1 |

## （一）安全托管服务要求

1、本次安全运营服务周期为1年，供应商需充分利用我院现有安全工具，对我院至少50个资产对象进行7\*24h安全专家线上值守，做到实时监测，并依据要求的服务水平SLA进行事件响应与处置；

2、供应商所提供的运营服务平台需支持与我院现有安全组件防火墙、行为管理、终端防护组件和态势感知平台做对接，或在中标一周内完成运营平台与我院现有安全组件的对接，以保证采集的安全日志和数据尽可能全面。

3、为我院提供安全运营服务平台1年的使用权限，所提供的平台需能满足：

(1)支持面向我院的安全态势展示，展示出当前我院遭受的威胁事件信息以及脆弱性信息统计，并支持服务专家按照资产类别、威胁类型进行定制化筛选查看，能直观感受到医院当前的风险态势情况。（注：提供服务平台漏洞表、事件表统计信息截图，并证明支持按照资产类别、威胁类型进行定制化筛选查看）

(2)本次采购的安全服务支持面向医院的安全报告与交付物管理，可生成、导出、下载各类安全报告，包括但不限于《安全服务值守日报》、《特殊时期值守报告》、《安全运营周报》、《安全运营月报》。（注：供应商提供支持上述交付物管理界面的截图）。

(3)业务安全状态监控：提供服务监控门户（或用户Portal，区别于安全感知大屏），在门户中我院可查看业务和资产安全状态信息，使得我院能直观感受到当前的业务和资产安全状态，展示纬度至少包括服务资产安全评级、服务运营状态及成果、安全风险概览、最新情报。

4、依托于服务工具需提供勒索病毒专项防护能力，能够直观展示勒索病毒防护效果，如已拦截阻止的勒索行为，已成功处置的勒索病毒事件等。

5.提供挖矿病毒扫描工具，支持基于内存或进程等扫描挖矿病毒的相关信息。

6.支持将检测出来的恶意文件事件、暴力破解事件、微隔离事件的日志上报到已建设安全态势感知平台，并在安全态势感知平台进行分析和展示。

7.提供可视化的攻击溯源功能， 直观展示攻击链与入侵路径，便于及时发现潜在威胁。

8、资产动态识别与管理。供应商需结合安全工具发现的资产信息，对服务范围内资产的全面梳理，并在后续服务过程中对资产的存活性进行7\*24h的探测，当资产发生变更时，安全专家第一时间对变更信息进行确认与更新，避免出现资产不受监管的情况。

9、至少一次全面深度风险评估。供应商需针对我院单位内所有信息化资产进行全方位、深层次的安全风险评估，包括但不限于如下内容：脆弱性评估、基线配置核查、蠕虫病毒事件、失陷主机分析、挖矿病毒事件分析、潜伏威胁分析、攻击行为评估等。供应商需针对发现的问题协助院方进行处置，包含内网脆弱性问题，病毒类事件，入侵行为，勒索、挖矿类事件等；

10、供应商需提供每月一次针对服务范围内的资产的系统脆弱性和Web漏洞进行全量扫描，并针对发现的脆弱性进行验证，验证脆弱性在已有的安全体系发生的风险及分析发生后可造成的危害，供应商需提供安全运营平台工具，对脆弱性进行全生命周期的可视化管理闭环。具体需满足：

(1)针对发现的脆弱性需提供客观的修复优先级指导，不能以脆弱性危害等级作为唯一的修复优先级排序依据。排序依据包含但不限于资产重要性、漏洞等级以及威胁情报（漏洞被利用的可能性）三个维度；

(2)提供脆弱性验证服务，针对发现的脆弱性问题进行验证，验证脆弱性在已有的安全体系发生的风险及分析发生后可造成的危害。针对已经验证的脆弱性，自动生成工单，安全专家跟进修复状态，各个处理进度透明，方便我院清晰了解当前脆弱性的处置状态，将脆弱性处理工作可视化；

(3)针对服务平台生成的工单，我院可按需催单，用户可在服务平台上采用邮件等方式提醒安全专家加快协助处置，督促供应商第一时间处理；

(4)需提供脆弱性复测措施，及时检验脆弱性真实修复情况。供应商要支持我院可按需针对指定脆弱性问题，指定资产等小范围进行，降低脆弱性复测时的潜在影响范围；

(5)对发现的脆弱性建立状态总览机制，自动化持续跟踪脆弱性情况，清晰直观地展示脆弱性的修复情况，遗留情况以及脆弱性对比情况，使得我院可做到脆弱性的可视、可管、可控；

(6)最新漏洞预警与排查：供应商需实时抓取互联网最新漏洞与详细资产信息进行匹配，对最新漏洞进行预警与排查。预警信息中包含最新漏洞信息、影响资产范围。一旦确认漏洞影响范围后，供应商需提供专业的处置建议，处置建议包含两部分，修复方案以及临时规避措施，并对该最新漏洞建立工单进行持续跟踪。

11、需对我方的网络提供7\*24H实时在线威胁监测与响应，从攻防视角出发帮助用户做好持续性攻击监测，主动防御外界的威胁，并及时进行处置。具体要求如下：

（1）7\*24H威胁监测与通告：依托于安全防护组件、检测响应组件等安全设备和大数据处理平台，将海量的威胁情报，攻击日志和异常流量进行数据关联分析，发现各类安全事件，实时监测网络安全状态，在安全运营管理平台上对攻击事件自动生成工单。攻击事件包含境外黑客攻击事件、暴力破解攻击事件、持续攻击事件；

1. 实时攻击对抗：通过全网大数据分析，当发现有持续性攻击、病毒入侵、境外黑客或高级黑客攻击，供应商需能联动用户现有安全设备，第一时间采取行动实时对抗黑客行为（如封锁黑客攻击IP）。

（3）威胁分析与处置：供应商需针对每一类威胁，进行深度分析验证，分析判断是否存在可疑主机，将深度关联分析的结果通过邮件、微信等方式告知用户。针对分析结果提供对应的处置或加固建议（如封锁攻击源、设置安全策略防护等措施）

（4）流行威胁通告与排查：结合威胁情报，供应商需排查是否对服务资产造成影响并通知用户，及时协助进行安全加固。

12、供应商需能对用户上报的安全事件及主动检测到的安全事件进行及时响应，对通过工单对安全事件的全生命周期进行管理。具体需满足：

（1）实时针对异常流量、攻击日志和病毒日志进行分析，聚合发现安全事件。针对分析得到的安全事件，基于主动响应和被动响应流程，对页面篡改、通报、断网、webshell、黑链等各类严重安全事件进行紧急响应和处置的解决方案，并通过工单系统跟踪处置情况。

（2）应急响应：全年不限次数向用户提供应急响应服务。根据安全事件的实际情况，先对入侵影响进行抑制，通过事件检测分析，提供抑制手段，降低入侵影响，协助快速恢复业务；再排查攻击路径，清除相关恶意文件；并还原攻击路径，分析入侵事件原因；最后结合现有安全防御体系，指导用户进行安全加固、提供整改建议、防止再次入侵。

13、需对安全事件服务水平作出承诺：

（1）从安全日志产生到事件通告给我院的时间方面，重大安全事件通告时间小于30分钟，一般事件的通告时间少于1小时。

（2）运营服务对于重大安全事件的遏制影响和处置完成时间小于1小时，对于一般事件的遏制影响和处置完成时间小于4小时。

（3）安全事件经过服务人员的确认后，各类安全事件的判断准确率不低于99%。

（4）安全事件的闭环处置比例达到100%。

（5）对于重大事故应启动应急响应机制，15分钟之内云端专家进行响应，2小时上门处置。

14、需对安全威胁服务水平作出承诺：

（1）从安全日志产生到威胁通告给我院的时间方面，重大威胁的通告时间少于1小时，一般威胁的通告时间少于2小时。

（2）高级威胁的处置完成时间少于1小时，一般威胁的处置完成时间少于4小时；

（3）安全威胁经过服务人员的确认后，高级威胁和一般威胁的判断准确率不低于99%。

（4）高级威胁和一般威胁的闭环处置比例达到100%。

15、服务期间服务交付物要求如下：

交付物名称：《安全服务运营报告》，报告频率：每周一次

交付物名称：《首次威胁分析与处置报告》，报告频率：一次

交付物名称：《事件分析与处置报告》，报告频率：按需触发，不限次数

交付物名称：《安全通告》，报告频率：按需触发，不限次数

交付物名称：《综合分析报告/运营月报》，报告频率：每月一次

交付物名称：《季度汇报PPT》，报告频率：每季度一次

交付物名称：《年度汇报PPT》，报告频率：每年一次

1. 中标后我院有权要求供应商严格按照上述频率要求提供服务交付物，确保满足我院安全需求。如供应商未能按时提供，我院有权终止服务合同，中间产生任何费用由供应商自行承担。（注：需提供相应交付物模板或样例）

## （二）渗透测试服务要求

1、我院授权后，供应商应提供两次通过模拟黑客攻击行为通过本地或远程方式对目标对象进行非破坏性的入侵测试。

2、渗透测试应至少包括但不限于以下范围的漏洞：

WEB应用系统渗透

主机操作系统渗透

数据库系统渗透

3、渗透测试内容包括但不限于：

身份验证类

会话管理类

访问控制类

输入处理类

信息泄露类

第三方应用类

4、供应商渗透测试人员应针对使用不同技术手段发现不同纬度的漏洞，并进行验证，形成记录和报告

5、供应商应编写渗透测试报告并提交给我院，报告应该阐明我院业务系统中存在的安全隐患以及专业的漏洞风险处置建议。

6、供应商应在投标文件技术部分详细说明渗透测试的实施流程、渗透测试方法、实施过程中用到的工具、实施过程中可供考量的具体工作指标及各阶段输出成果。

服务交付物：《渗透测试报告》

## （三）红队检测（攻防演练）

一服务要求

红队检测服务包含以APT攻击者视角对医院目前现有防御措施进行深度渗透测试，对目标系统、人员、软硬件设备、基础架构，进行多维度、多手段、对抗性模拟攻击，旨在发现可能被入侵的薄弱点，并以此为跳板将攻击渗透结果最大化（包括系统提权、控制业务、获取信息），进而检验现有防御体系的短板。

二服务内容

1前期确认阶段服务商与医院进行沟通、确定红队检测的时间、范围、目标系统、深度、测试方式（现场或者远程）等问题，并拿到医院签署的红队检测授权函。

2情报搜集阶段针对基础资产、互联网信息泄露、指纹识别、系统业务功能、移动端接口信息、典型边界二次梳理等情报收集。

3外围打点阶段红队攻击队员根据情报收集阶段获取到的信息进行综合分析，对业务系统从不同维度开展试探性攻击。

4远程社工阶段通过钓鱼邮件、欺诈短信、假冒身份、社工库、鱼叉邮件、交友诈骗、水坑攻击等社工方式进行攻击。

5近源攻击阶段通过伪造WiFi钓鱼、BadUSB、虚假活动钓鱼等方式获取员工敏感个人信息，开展身份识别绕过、本地网络嗅探、硬件系统漏洞利用、树莓派接入评估等安全检测手段。

6内网渗透阶段通过内网敏感信息收集进行内网横向渗透，利用主机权限和专有数据信息获取目标系统权限，以此评估内网整体安全性。

7报告输出阶段红队检测工作全部完成后输出《红队检测报告》，报告中阐明医院网络中存在的安全隐患以及专业的风险处置建议。

8汇报阶段红队检测工作结束后，项目经理配合医院及相关技术人员，对本次红队检测工作中获得的成果、经验以及需要改进的问题进行总结汇报。

三 服务需要交付物

《红队检测项目实施风险告知书》、《SFSS-RTP-F0002安全服务保密协议》、《SFSS-RTP-F0003红队检测服务启动函》、《SFSS-RTP-R0101 红队检测报告》、《SFSS-RTP-T0101红队检测服务实施方案》

# ❷、IT核心机房运维技术要求

## （一）、IT核心机房运维设备情况

|  |  |  |
| --- | --- | --- |
| 设备类型 | 合计数量 | 启用时间 |
| 2018年前 | 2018-2020 | 2021-2023 |
| 服务器及存储 | 47 | 20 | 3 | 24 |
| 网络设备 | 110 | 75 | 22 | 13 |
| 服务期内甲方购买的新设备 | 不限 |  |  |  |

## （二）、IT核心机房运维服务要求

为都江堰人民医院提供硬件设备（包括第三方配套软件）技术支持服务，处理相关系统技术问题，紧急故障响应，提供维护保障；承担运维服务的业务管理和协调工作，确保医院信息系统7×24小时正常运行。具体运维要求及标准如下：

1、资产台账建设服务：对运维设备进行资产台账的建设，包括资产台账的及时创建、更新、动态维护等。

2、数据中心核心硬件设备安全运行保障服务：定期对网络设备配置进行备份，定期对数据中心核心硬件设备进行数据备份的巡检和校验；

3、硬件设备配置管理服务：整理记录当前硬件架构中所有最新的，准确的，全面的和详细的信息配置，并管理其变更，使这些信息有效而高效地支持其它流程运行；

4、巡检服务及报告服务：提供本地化服务团队，并提供以下服务：

①每月定期对机房例行巡检并提供例行巡检报告;

②每月对机房设备运行状态巡检并记录报告;

③每半年进行一次运维工作总结，并提交报告书;

④每次故障处理后填写记录表;

⑤每月全面健康性检查，全面检查设备系统的工作状态，总结本月的故障处理事项，作月报记录；

5、设备资产标标识标签基础维护管理服务：针对设备以及机房网络链路的标识标签管理、维护和更新。

6、故障处理服务：重大故障事件须提供现场保障服务，并在故障处理完毕3个工作日内提供相应的故障分析报告，对故障现象、故障处理经过和故障处理结果进行描述，包括故障原因分析和相关改进建议等；

7、应急措施服务：针对各项应急故障、做好应急措施；定期（每半年一次）开展应急演练；

8、本次运维项目部分所涉及的服务内容为整体包干服务，所有人工、配件费用都包含在成交价格内，不另行结算，采购人不再支付额外费用。在设备的运维周期内，应保证更换到原厂的设备配件，确保设备的正常使用。

1. 其他服务：运维设备使用中经常出现的问题进行梳理，并对其定期开展培训服务直至问题得以解决。同时提供技术咨询服务。
2. 服务要求

①服务人员及工作时间：

法定工作日每天8:00-18:00至少1人驻场运维；18:00至次日8:00及节假日至少1人电话值班运维，受理服务请求或帮助甲方解决技术问题。

②故障响应要求：

根据故障的严重程度和影响程度的不同，故障级别由低到高分为三级故障、二级故障、一级故障。当故障没有在规定时限内恢复或解决时，故障级别将自动升级。

一级故障（重大故障）：指设备或软件在运行中出现系统瘫痪或服务中断，导致设备的基本功能不能实现；其他造成业务中断30分钟小时以上或导致关键业务数据丢失的故障。

二级故障（主要故障）：指设备或软件在运行中出现的直接影响服务，导致系统性能或服务能力部分丧失的故障；设备或软件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，并可能导致设备或软件基本功能不能实现，如冗余设备单侧故障等；系统设备或操作系统故障，造成业务中断但不满2小时的，如系统复位等；

三级故障（次要故障）：指设备或软件在运行过程中出现的，影响系统功能和性能，但关键业务不受影响的故障。

故障响应要求：

|  |  |
| --- | --- |
| 故障级别 | 服务描述 |
| 一级故障 | 7\*24小时接受报障，工作时间15分钟内现场响应，非工作时间2小时内现场响应 |
| 二级故障 | 7\*24小时接受报障，工作时间1小时内现场响应，非工作时间4小时内现场响应 |
| 三级故障 | 7\*24小时接受报障，48小时内现场响应 |

## （三）、IT核心机房运维需续保设备清单

## 安全设备三年过保后硬件维保购置及软件升级购置（2024年5月过保）

|  |  |  |  |
| --- | --- | --- | --- |
| 序号 | 型号 | 数量 | 备注 |
| 1 | AF-1000-B1800 | 2 | 产品质保、软件升级、深信服云智订阅软件（AF8.0.7及以上版本适用） |
|
| 2 | DAS-1000-A620S | 1 | 产品质保、软件升级(DAS-1000-A620S) |
| 3 | AC-1000-B1400 | 1 | 产品质保、软件升级、URL&应用识别规则库软件升级 |
|
| 4 | AF-1000-B1400 | 2 | 产品质保、软件升级、深信服云智订阅软件（AF8.0.7及以上版本适用）、深信服云鉴订阅软件（AF8.0.7及以上版本适用） |
| 5 | OSM-1000-B1150 | 1 | 产品质保、软件升级（OSM-1000-B1150） |
| 6 | STA-100-B2100 | 1 | 产品质保、软件升级、深信服安全感知系统探针特征库软件V2.0 |
|
| 7 | SIP-1000-F600 | 1 | 产品质保、软件升级、深信服安全感知系统平台特征库软件V2.0 |
|
| 8 | LAS-1000-C600 | 1 | 产品质保、软件升级 |
| 9 | BVT-1000-B1150 | 1 | 产品质保、软件升级 |
| 10 | EDR | 1 | 软件升级 |

## 云管理平台软件原厂软件升级更新续保（ZStack Cloud）（2023年9月过保）

ZStack Cloud技术支持服务：24C原厂Cloud年度技术支持服务)服务内容：1. 400电话、工单系统远程(5\*8小时支持服务；2. 1年期云平台的在线升级更新服务；3. 云平台使用的使用指导和使用帮助；4. 云平台使用的定期巡检，巡检报告；5. 云平台使用的远程故障排查。

## 虚拟化存储软件三年过保后维保购置原厂软件升级续保（xsky）（2023年1月过保）

xsky技术支持服务：12C原厂Cloud年度技术支持服务)服务内容：1. 400电话、工单系统远程(5\*8小时支持服务；2. 1年期虚拟化平台的在线升级更新服务；3. 虚拟化平台使用的使用指导和使用帮助；4. 虚拟化平台使用的定期巡检，巡检报告；5. 虚拟化平台使用的远程故障排查。

## 云平台计算资源服务器6+1台（曙光H620-G30）三年过保续保购置原厂核心部件更换

|  |  |  |  |
| --- | --- | --- | --- |
| 型号 | 序列号 | 出厂日期 | 保修结束日期 |
| H620-G30 | 9800169903134553 | 2021年11月23日 | 2024年12月23日 |
| H620-G30 | 9800169903134548 | 2021年11月23日 | 2024年12月23日 |
| H620-G30 | 9800169903134552 | 2021年11月23日 | 2024年12月23日 |
| H620-G30 | 9800169903134549 | 2021年11月23日 | 2024年12月23日 |
| H620-G30 | 9800169903134546 | 2021年11月23日 | 2024年12月23日 |
| H620-G30 | 9800169903134551 | 2021年11月23日 | 2024年12月23日 |
| H520-G30 | 9800129702560734 | 2021年11月23日 | 2024年12月23日 |

## 存储系统计算节点3台（曙光H620-G30）三年过保续保购置原厂核心部件更换

|  |  |  |  |
| --- | --- | --- | --- |
| 型号 | 序列号 | 出厂日期 | 保修结束日期 |
| H620-G30 | 9800127302015390 | 2019/12/18 | 2023/1/17 |
| H620-G30 | 9800127302015391 | 2019/12/18 | 2023/1/17 |
| H620-G30 | 9800127302015392 | 2019/12/18 | 2023/1/17 |

# ❸信息化硬件终端运维服务

## （一）维护保养及维修服务范围

1、服务对象为都江堰市人民医院现有科室所有信息化硬件维护。

2、计算机系统软件维护：操作系统、办公软件、杀毒软件等常用软件安装、 配置、更新及问题处理、技术支持；医院专用软件的客户端程序安装配置。

3、硬件设备包含但不限于如下设备：台式计算机、便携式计算机、打印机、复印机、多功能一体机、条码打印机、投影仪等各类信息化设备硬件的维护:安装调试、保养、维修等。现有相关主要设备如下表：

|  |  |  |
| --- | --- | --- |
| 设备类型 | 合计数量 | 启用时间 |
| 2018年前 | 2018-2020 | 2021-2023 |
| 计算机终端 | 1200 | 260 | 241 | 699 |
| 打印设备 | 689 | 202 | 209 | 278 |
| 复印机 | 7 | 4 | 1 | 2 |
| 投影仪 | 15 | 5 | 4 | 6 |
| 服务期内甲方购买的新设备 | 不限 |  |  |  |

4、网络线路和设备维护：网络终端点故障处理、网络线路的规范梳理及网络设备的安装调试、检修等。

5、设备巡查维护：定时对各类信息化硬件设备进行巡查，及时处理发现的问题并与相关科室做好沟通记录，最后形成完整的巡查记录电子文件。

6、本次硬件服务终端运维项目部分所涉及的服务内容为整体包干服务，所有人工、配件费用都包含在成交价格内，不另行结算，采购人不再支付额外费用。

## （二）人员配置及维修维护要求

**一、人员配置要求**

1、配备驻点运行维护人员3名，要求驻点人员具有专科及以上学历，具有3年以上IT行业工作经验。

2、驻点人员需到信息管理部备案并统一制作挂牌上岗。未经医院同意，不得私自撤离和随意更换。对于技术水平低、服务态度差、工作不认真、责任性不强的维护人员，在医院提出更换要求下，需立即予以更换。

3、日常维护期间，必须提供不少于3名的专业维护人员，进行7\*24小时驻点服务，按甲方作息时间上下班, 夜间要有人员与电话值班方式保障甲方业务正常开展的需求，周末及节假日不得少于1人响应服务，如遇任务繁重时应及时加派人手，以保证业务的正常运作及开展。

4、当设备出现故障时要及时处理，驻点维护人员有熟练的现场故障处理能力，将故障处理时间控制在30分钟内。不能现场处理的故障机器要及时用备用机器替换，并保证在承诺的时间内修复故障设备。

5、供应商必须负责全院所有电脑、打印机等信息类设备的终端维护维修，并保证所有设备正常运行；同时要每季巡查所有设备运行情况并登记，同时将巡查结果交医院，保证所有设备正常运行。

6、每季度在全院科室开展一次满意度调查，服务质量严格按考核要求执行。

## （三）维护维修服务工作具体要求

一、维护内容：

定期报告提交运行维护季度报、全年工作总结，主要内容包含：

1、重大事件通报（事件分类及汇总，详细清单）

2、故障分析（故障分类，故障简述，原因，发生时间，解决问题时间，解决程度与解决方法，影响范围和详细清单）

3、故障类型分类统计

4、硬件系统和软件系统配置版本更新情况

5、日常维护问题汇总，并根据问题类型，编制一般性问题的解决办法与维护文档。

6、一些即将达到阈值的系统进行提示，便于专业技术组进行相应的维护。

7、对于预防性维护的记录和即将发生的维护进行提示。

二、日常监控：

1、维护部门应按照计划，安排符合要求的专业技术人员。对计算机终端、打印机设备状态进行监控，对发现的故障、系统提示、运行性能、资源占用情况等重要事件进行分析和处理。

三、预防性维护与巡检：

维护部门应按照计划进行巡检，由专业技术人员定期和不定期现场维护或远程维护，针对正常运行的设备、应用软件、系统软件进行全面检查，对可能发生的故障进行排除。

1、定期进行设备测试检查,找出隐患,尽早排除。

2、定期进行设备的清洁保养。

3、对于系统性能问题予以调整，并在必要时提出升级计划。

4、及时向主管人员汇报设备状态的第一手信息。

5、提供定期巡检维护服务：对各设备信息化硬件设备运行状态进行每日至少一次全面巡检；对各类服务器、存储、交换机、重要信息化设备的运行状态每周至少一次全面巡检；对各类计算机、打印机、复印机等常规信息化设备的运行状态进行每季至少一次全面巡检。在巡检过程中应与相关科室做好沟通记录，所有巡检完成后应形成书面形式的巡检记录，同时提供便于统计、查询的电子日志。

6.每次服务完成后服务人员必须提供相关服务单据及电子日志给相关科室确认，同时电子日志具有在线实时查询单个故障设备一年内历史维修记录的功能。

四、版本升级与增强：

1、在设备相关软件需要升级时，首先维护人员从供应商那里取得要更新的软件在信息中心模拟环境下进行测试，确保正确。

五、设备维修：

1、设备在运行过程中发生物理故障，如电源、风扇故障，板卡、硬盘、马达、齿轮故障等。维护人员在监控或接到设备报障后，应记录故障信息，并确认是否需要更换配件，需要更换配件的现场免费更换。

2、如确认配件需要更换或返厂维修，需要填写申请表。申请表需详细描述故障现象、处理意见、返回时间等内容。

3、主机设备系统维护，维护人员应首先与使用人协商一致，做好备份等保障操作后，按照相关要求执行，执行完毕应按照日常维护要求进行记录。

4、无法在现场及时修复的故障，供应商需在规定时间内提供与故障硬件相同功能的顶替备用机，保证医院工作的正常开展。供应商应提供满足医院使用需求的备用机，且数量不低于清单中列举的数量。

|  |  |  |  |
| --- | --- | --- | --- |
| 序号 | 名称 | 数量 | 单位 |
| 1 | 台式计算机 | 5 | 台 |
| 2 | 便携式计算机 | 1 | 台 |
| 3 | 激光打印机 | 5 | 台 |
| 4 | 票据打印机 | 2 | 台 |
| 5 | 标签打印机 | 2 | 台 |

5、设备确已无法维修，由现场人员申请，交由信息管理部按办公设备相关使用规定审核确认后，再按医院流程办理。

6、维保更换配件（产品）必须是具备正规合法经销渠道的，符合国家各项有关质量标准及采购质量标准的合格产品。

附件（报价单）：

|  |
| --- |
| **报价单** |
| **序** | **项目名称** | **单位** | **报价（元）** |
| 1 | 信息安全服务 | 安全托管服务 | 年 | 　 |
| 2 | 渗透测试服务 | 年 | 　 |
| 3 | 攻防演练 | 次 | 　 |
| 4 | IT核心机房运维 | IT核心机房运维服务 | 年 | 　 |
| 5 | 安全设备续保 | 年 | 　 |
| 6 | 云管理平台续保 | 年 | 　 |
| 7 | 虚拟化存储软件续保 | 年 | 　 |
| 8 | 云平台计算资源服务器续保 | 年 | 　 |
| 9 | 存储系统计算节点续保 | 年 | 　 |
| 10 | 信息化硬件终端运维服务 | 信息化硬件终端运维服务 | 年 | 　 |