**延安市中医医院关于机房安全运维服务项目**

**内容及技术要求**

**一、背景描述**

我院信息化发展迅速，各系统设备原厂质保周期短，部分信息化设备和机房环境设备均已过保，系统的连续性和稳定性运行无法得到保障。通过运行维护服务的有效管理来提升信息系统的服务效率，提高服务质量。结合我院现有的组织结构、系统资源和管理流程的特点，从流程、人员和技术三方面来规划我院信息系统运维模式，以达到医院快速发展的要求。

**二、现状分析**

医院中心机房设备种类丰富，数量众多。网络及安全设备策略复杂繁琐。如要维护好机房内所有设备及其相关策略，会花费大量的人力资源。且机房系统是顶层业务的基础物理环境。要保证业务稳定连续行，就要保证底层基础环境稳定。

现有设备多数都已使用三年以上且大多数已超过产品保修期，医院现有IT技术员能对核心设备做基本的管理和使用，但核心设备其专业性较强，部分设备出现故障，需要专业技术人员调试解决。医院管理使用人员无法做到及时处置设备故障。若设备出现故障之后去联系厂家解决时，厂家单次维修成本较高。且会延长故障周期，容易造成因硬件设备故障造成的数据丢失或者业务异常。综上所述，我院对信息化设备的运维服务的需求以迫在眉睫。

具体设备清单如下：

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 序号 | 名称 | 品牌 | | 型号 | 数量 | 单位 | 备注 |
| **网络设备** | | | | | | |  |
| 1 | 内网核心交换机 | | 华为 | S12708 | 2 | 台 |  |
| 2 | 内网汇聚交换机 | | 华为 | S7706 | 4 | 台 |  |
| 3 | 出口路由器 | | 华为 | AR3260 | 1 | 台 |  |
| 4 | 外网核心交换机 | | 华为 | S7706 | 1 | 台 |  |
| 5 | 外网汇聚交换机 | | 华为 | S7706 | 1 | 台 |  |
| 6 | 出口路由器 | | 华为 | AR3260 | 1 | 台 |  |
| 7 | 接入交换机 | | 华为 | S5720 | 194 | 台 |  |
| 8 | 无线 AC 控制器 | | 华为 | AC6605-26-PWR | 2 | 台 |  |
| 9 | 无线 AP | | 华为 | AP4050DN | 192 | 台 |  |
| 10 | POE 交换机 | | 华为 | S5720POE | 13 | 台 |  |
| 11 | 内网无线Ap | | 华为 | R240A | 494 | 台 |  |
| 12 | AD | | 华为 | AD9430DN-24 | 22 | 台 |  |
| 13 | Esight管理系统 | | 华为 | V300R006 | 1 | 套 |  |
| **安全设备** | | | | | | |  |
| 1 | 外网下一代防火墙 | 深信服 | | AF-1800-EI | 1 | 台 |  |
| 2 | 外网上网行为管理设备 | 深信服 | | AC-1800-EI | 1 | 台 |  |
| 3 | 外网 web 应用防护系统 | 深信服 | | AF-1580-WAF | 1 | 台 |  |
| 4 | 内网入侵检测及防病毒设备 | 深信服 | | AF-1850-AV | 1 | 台 |  |
| 5 | 内网下一代防火墙 | 深信服 | | AF-1800-EI | 1 | 台 |  |
| 6 | 内网数据库安全审计 | 深信服 | | DAS-4300-EI | 1 | 台 |  |
| 7 | 内网堡垒机 | 帕拉迪 | | PLDSEC SMS 6500ST-AS2-Pro | 1 | 台 |  |
| 8 | 内网应用性能分析管理设备 | 深信服 | | APM-4200 | 1 | 台 |  |
| 9 | 内网服务器负载均衡 | 深信服 | | AD-2000-EI | 1 | 台 |  |
| 10 | 主机审计系统 | 北信源 | | V6.6 | 1 | 台 |  |
| **服务器、存储、备份、虚拟化设备** | | | | | | |  |
| 1 | 虚拟化服务器 | 浪潮 | | NF8465M4 | 4 | 台 |  |
| 2 | 虚拟化软件 Vmware | 浪潮 | | InCloud SphereV4.5 旗舰版 | 1 | 台 |  |
| 3 | 存储 | 浪潮 | | AS520E-M1 | 2 | 台 |  |
| 4 | 光纤交换机 | 浪潮 | | FS5900 | 2 | 台 |  |
| 5 | 备份一体机 | 浪潮 | | DP1000-M1 | 1 | 台 |  |
| 6 | HIS服务器1 | 浪潮 | | NF8465M4 | 1 | 台 |  |
| 7 | HIS服务器2 | 浪潮 | | NF8465M4 | 1 | 台 |  |
| 8 | 排队叫号系统服务器 | 联想 | | RD450 | 1 | 台 |  |
| 9 | 医护对讲系统服务器 | 浪潮 | | NF5270M4 | 1 | 台 |  |
| 10 | 原 HIS 服务器（利旧） | IBM | | X3650 M4 | 1 | 台 |  |
| 11 | 用友财务软件服务器（利旧） | HP | | ML330 G6 | 1 | 台 |  |
| 12 | 延安市医保前置服务器（利旧） | IBM | | X3650 M4 | 1 | 台 |  |
| 13 | 延安市卫生计生信息平台前置服务器（利旧） | 浪潮 | | NF-5280M4 | 1 | 台 |  |
| 14 | 银行前置服务器 | 联想 | | SR590 | 1 | 台 |  |
| 15 | 自助机服务器 | 联想 | | SR590 | 1 | 台 |  |
| 16 | 中联交互/医保支付 | 联想 | | SR590 | 1 | 台 |  |
| 17 | 微信支付宝服务器 | 联想 | | SR590 | 1 | 台 |  |
| 18 | HIS双机软件 | 浪潮 | | ROSE HA | 1 | 套 |  |
| 19 | 2路服务器 | 浪潮 | | NF5280M5 | 1 | 套 |  |
| 20 | 虚拟化服务器 1 | 紫光华山 | | HPE DL580Gen10 | 4 | 台 |  |
| 21 | 虚拟化软件 | VMware | | 6.7 | 1 | 套 |  |
| 22 | 虚拟化服务器 2 | 紫光华山 | | HPE DL380Gen10 | 10 | 台 |  |
| 23 | 磁盘阵列 | 紫光华山 | | HPE 3PAR 8200 | 1 | 台 |  |
| 24 | 光纤通道交换机 | 紫光华山 | | HPE SN3000B | 2 | 台 |  |
| 25 | PACS存储 | 浪潮 | | AS2150G2 | 1 | 台 |  |
| **机房基础环境设备** | | | | | | |  |
| 1 | 空调 | 世图兹 | | CPD 622A | 4 | 台 |  |
| 2 | UPS及电池 | 艾默生 | | APM 150 | 2 | 套 |  |
| 3 | 动环系统 | 计通 | | Industrial Computer 510 | 1 | 套 |  |
| 4 | 七氟丙烷 | 海湾 | | GST | 5 | 台 |  |
| 5 | 统一时钟 | 上海凌通 | | PN20A | 2 | 台 |  |

**三、运维服务方案设计**

**1、服务目标**

机房安全运维服务的目标是，对我院中心机房、汇聚机房、弱电机房、病房呼叫系统等现有的信息系统基础资源进行监控、管理和维护，及时掌握网络信息系统资源现状和配置信息，反映信息系统资源的可用性情况和健康状况，创建一个可知可控的IT环境，从而保护信息系统的各类业务应用系统的可靠、高效、持续、安全运行。升级安全杀毒软件、对信息系统进行等保测评。

运维项目提供专业可靠的服务，包含但不限于以下内容：

（1）保障设备的稳定性和可靠性；

（2）保障设备的安全性和可恢复性；

（3）故障的及时响应与修复；

（4）硬件设备的维修与更换服务；

（5）人员的技术培训服务；

（6）应急预案的制定及演练；

（7）信息化建设规划、方案制定等咨询服务。

通过机房设备维护保养可以提高设备的使用寿命，降低设备出现故障的概率，避免重特大事故发生，避免不必要的经济损失。设备故障时，可提供快速的备件供应，技术支持，故障处理等服务。通过系统的维护可以提前发现问题，并解决问题。将故障消灭在萌芽状态，提高系统的安全性，减少人力、物力投入的成本。为机房内各系统及设备的正常运行提供安全保障。可延迟设备的淘汰时间，使可用价值最大化。通过引入专业的维护服务，可以将管理人员从日常需要完成专业性很强的维护保养工作中解放出来，提升工作效率，更好的发挥信息部门的自身职能。通过专业的维护，将机房内所有设备的运行数据进行整理，进行数据分析，给机房基础设施建设、管理和投入提供依据。

为保证我院系统应用的业务连续性，考虑机房现有设备维保情况。为关键网络设备和存储、安全设备、不间断电源设备、备份系统以及服务器虚拟化提供一个综合性的维护服务，包括硬软件，最大限度减少信息化系统的非计划停机的可能性及突发故障的发生；在故障发生时，保障备件的快速更换和系统软件的快速恢复，最大限度地减少系统停机的持续时间。

**2、运维服务范围**

机房安全运维服务范围主要有中心机房、汇聚机房、弱电机房设施设备运维服务（配件更换+驻场运维+故障处理服务+技术支持）、专业安全服务、主要硬件设备维保服务、信息化建设咨询服务等。

我院机房内的服务器、存储、网络、安全、机房环境设备，并且包括设备的操作系统、数据库、中间件、备份软件、虚拟化软件等机房内所有设备。设备清单如下但不局限于；

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 序号 | 名称 | 品牌 | | 型号 | 数量 | 单位 | 备注 |
| **网络设备** | | | | | | |  |
| 1 | 内网核心交换机 | | 华为 | S12708 | 2 | 台 |  |
| 2 | 内网汇聚交换机 | | 华为 | S7706 | 4 | 台 |  |
| 3 | 出口路由器 | | 华为 | AR3260 | 1 | 台 |  |
| 4 | 外网核心交换机 | | 华为 | S7706 | 1 | 台 |  |
| 5 | 外网汇聚交换机 | | 华为 | S7706 | 1 | 台 |  |
| 6 | 出口路由器 | | 华为 | AR3260 | 1 | 台 |  |
| 7 | 接入交换机 | | 华为 | S5720 | 194 | 台 |  |
| 8 | 无线 AC 控制器 | | 华为 | AC6605-26-PWR | 2 | 台 |  |
| 9 | 无线 AP | | 华为 | AP4050DN | 192 | 台 |  |
| 10 | POE 交换机 | | 华为 | S5720POE | 13 | 台 |  |
| 11 | 内网无线Ap | | 华为 | R240A | 494 | 台 |  |
| 12 | AD | | 华为 | AD9430DN-24 | 22 | 台 |  |
| 13 | Esight管理系统 | | 华为 | V300R006 | 1 | 套 |  |
| **安全设备** | | | | | | | 深信服设备提供原厂服务，提供原厂授权书及售后服务承诺函 |
| 1 | 外网下一代防火墙 | 深信服 | | AF-1800-EI | 1 | 台 |  |
| 2 | 外网上网行为管理设备 | 深信服 | | AC-1800-EI | 1 | 台 |  |
| 3 | 外网 web 应用防护系统 | 深信服 | | AF-1580-WAF | 1 | 台 |  |
| 4 | 内网入侵检测及防病毒设备 | 深信服 | | AF-1850-AV | 1 | 台 |  |
| 5 | 内网下一代防火墙 | 深信服 | | AF-1800-EI | 1 | 台 |  |
| 6 | 内网数据库安全审计 | 深信服 | | DAS-4300-EI | 1 | 台 |  |
| 7 | 内网堡垒机 | 帕拉迪 | | PLDSEC SMS 6500ST-AS2-Pro | 1 | 台 |  |
| 8 | 内网应用性能分析管理设备 | 深信服 | | APM-4200 | 1 | 台 |  |
| 9 | 内网服务器负载均衡 | 深信服 | | AD-2000-EI | 1 | 台 |  |
| 10 | 主机审计系统 | 北信源 | | V6.6 | 1 | 台 |  |
| **服务器、存储、备份、虚拟化设备** | | | | | | | 浪潮设备提供原厂服务，提供原厂授权书及售后服务承诺函 |
| 1 | 虚拟化服务器 | 浪潮 | | NF8465M4 | 4 | 台 |  |
| 2 | 虚拟化软件 Vmware | 浪潮 | | InCloud SphereV4.5 旗舰版 | 1 | 台 |  |
| 3 | 存储 | 浪潮 | | AS520E-M1 | 2 | 台 |  |
| 4 | 光纤交换机 | 浪潮 | | FS5900 | 2 | 台 |  |
| 5 | 备份一体机 | 浪潮 | | DP1000-M1 | 1 | 台 |  |
| 6 | HIS服务器1 | 浪潮 | | NF8465M4 | 1 | 台 |  |
| 7 | HIS服务器2 | 浪潮 | | NF8465M4 | 1 | 台 |  |
| 8 | 排队叫号系统服务器 | 联想 | | RD450 | 1 | 台 |  |
| 9 | 医护对讲系统服务器 | 浪潮 | | NF5270M4 | 1 | 台 |  |
| 10 | 原 HIS 服务器（利旧） | IBM | | X3650 M4 | 1 | 台 |  |
| 11 | 用友财务软件服务器（利旧） | HP | | ML330 G6 | 1 | 台 |  |
| 12 | 延安市医保前置服务器（利旧） | IBM | | X3650 M4 | 1 | 台 |  |
| 13 | 延安市卫生计生信息平台前置服务器（利旧） | 浪潮 | | NF-5280M4 | 1 | 台 |  |
| 14 | 银行前置服务器 | 联想 | | SR590 | 1 | 台 |  |
| 15 | 自助机服务器 | 联想 | | SR590 | 1 | 台 |  |
| 16 | 中联交互/医保支付 | 联想 | | SR590 | 1 | 台 |  |
| 17 | 微信支付宝服务器 | 联想 | | SR590 | 1 | 台 |  |
| 18 | HIS双机软件 | 浪潮 | | ROSE HA | 1 | 套 |  |
| 19 | 2路服务器 | 浪潮 | | NF5280M5 | 1 | 套 |  |
| 20 | 虚拟化服务器 1 | 紫光华山 | | HPE DL580Gen10 | 4 | 台 |  |
| 21 | 虚拟化软件 | VMware | | 6.7 | 1 | 套 |  |
| 22 | 虚拟化服务器 2 | 紫光华山 | | HPE DL380Gen10 | 10 | 台 |  |
| 23 | 磁盘阵列 | 紫光华山 | | HPE 3PAR 8200 | 1 | 台 | 提供原厂服务，提供原厂授权书及售后服务承诺函 |
| 24 | 光纤通道交换机 | 紫光华山 | | HPE SN3000B | 2 | 台 |  |
| 25 | PACS存储 | 浪潮 | | AS2150G2 | 1 | 台 |  |
| **机房基础环境设备** | | | | | | |  |
| 1 | 空调 | 世图兹 | | CPD 622A | 4 | 台 |  |
| 2 | UPS及电池 | 艾默生 | | APM 150 | 2 | 套 |  |
| 3 | 动环系统 | 计通 | | Industrial Computer 510 | 1 | 套 |  |
| 4 | 七氟丙烷 | 海湾 | | GST | 5 | 台 |  |
| 5 | 统一时钟 | 上海凌通 | | PN20A | 2 | 台 |  |

**3、服务内容**

**3.1信息资产统计服务**

资产统计服务为运维项目基本服务，帮助我们对现有的信息资产情况进行了解，更好的提供系统的运行维护服务。

服务内容主要包括但不限于：

（1）医院机房信息化硬件设备、中间件、数据库等型号、数量、版本、部署位置等信息统计形成文档记录。

（2）医院网络结构、网络路由、网络IP地址统计形成文档记录。

（3）绘制更新网络拓扑图和线路连接图统计形成文档记录。

（4）完成机房设施设备标签并粘贴、完成线缆标签并粘贴，形成文档记录。

（5）完成中心机房、汇聚机房、弱电机房线缆整理，保持标签清晰、线路整齐。

**3.2机房维护**

定期到用户现场对服务范围内设备进行巡检（每季度一次），保养、维护，对存在隐患的问题及时进行处置，确保设备处于安全、稳定运行状态，**并出具巡检报告**。

**3.2.1服务器、存储、备份一体机、虚拟化软件维护**

●**服务器、存储、备份一体机、虚拟化软件**

服务器系统主要包括目前在用的各类服务器：数据库服务器、应用服务器等；存储包括磁盘整列、光纤交换机；备份一体机；虚拟化软件：虚拟化平台、数据库。具体服务内容包括但不限于：

**1）服务器硬件部分：**

系统运行环境检查，包括机房温度、湿度和零地电压、零火电压等；

设备连接状况检查；

系统硬件运行情况检查；

系统LED数码检查分析；

对光驱和软驱做读写测试和必需的清洗；

系统运行状态、性能检查和优化，包括CPU、内存和交换区使用情况，硬盘和网络的IO情况检查；

记录系统存储空间的逻辑结构；

设备除尘处理；

检查如发现有隐患的部件将及时更换。

**2）服务器系统软件部分：**

软件版本或PTF实效性检查；

操作系统环境检查、安全检查、查看系统是否存在安全隐患，并及时修复；

系统错误日志分析；

超级用户邮件分析，清理过期邮件；

系统的安全性检查与防范；

文件系统空间使用情况检查；

系统运行状态、性能检查和优化情况检查；

记录系统存储空间的逻辑结构；

存储配置检查及有效性测试；

操作系统版本及微码检查；

系统备份的可用行和恢复性检查。

服务器更换常备部件主要如下但不限于：

CPU/内存/硬盘、主板/网口/光口、电源背板/电源模块、RAID卡（存储控制器）、RAID卡电池（电容）、风扇、Riser卡、PCI—E扩展卡硬盘背板、SAS线缆、IO框、交换模块。

现场更换部件，注意事项：

非热插拔部件更换需要中断业务，下电操作，需要取得客户正式授权方可进行。

单板、内存等PCB板/卡需要佩戴防静电手套操作。

CPU更换需要佩戴防静电腕带操作，不能佩戴防静电手套。

CPU更换时轻拿轻放，垂直于CPU底座拆装，不允许反复平移，避免造成CPU底座弯针（二次坏件）。

主板更换，涉及大客户及定制化客户的，需要核实相关软件（主要为iMana/BIOS版本）版本及定制化信息满足客户要求

**3)存储、备份设备维护**

存储系统平台主要包括但不限于：SAN存储系统（接入SAN网络的服务器客户端、SAN交换机）、磁盘阵列等的管理和维护工作。具体服务内容包括但不限于：

存储设备运行维护

记录与报告

存储设备具体巡检流程包括但不限于例如下：

设备登陆

状态检查

通过对以上各种设备的巡检旨在及时发现并消除设备运行过程中可能存在的缺陷或隐患，并采取适当的措施予以恢复和处理，维持设备的健康水平，降低设备的故障率。

实时掌握设备和网络的运行状况，了解设备和网络的运行趋势，提高维护人员对突发事件的处理效率。

通过定期维护和保养设备，使设备的健康水平长期处于良好状态，确保系统能够安全、稳定、可靠的运行。

通过定期检查、备份、测试、清洁等手段，及时发现设备在运行过程中出现的自然老化、功能失效、性能下降等缺陷，并采取适当的措施及时予以处理，以消除隐患，预防事故的发生。

提供存储、SAN交换机等设备的故障处理、维护及性能调优等，以保证本次维保的设备及所运行的系统正常运行。

备份系统维保服务

备份系统包括备份一体机，服务内容包括：

设备正常运行保障

对现有备份业务状态检测，熟练掌握备份系统的使用方法，对需要备份的应用，可正常配置备份业务并恢复测试，根据需求调整备份策略

**4）虚拟化系统维护**

虚拟化平台维护

现有VMware虚拟化平台和浪潮虚拟化平台，主要包括虚拟化管理平台、SAN交换机、物理节点、虚拟机等组件。具体服务内容包括：

云平台常规巡检

各虚拟化节点的巡检

云平台故障记录与报告

虚拟化平台巡检流程如下：

平台登陆

查看状态

数据库维护

数据库服务内容包括：

健康检查。

数据库工程师定期（最小频率为每季度1次）到用户现场，对数据库系统进行例行健康检查，并提交报告，根据健康检查的内容对数据库进行优化。检查的内容应包括但不限于以下内容：空间使用情况，日志，表空间，TOP，备份情况，运行状态等。

数据库及应用系统性能调优。

数据库及应用系统的性能调整一般包括，但不局限于如下内容：采集系统运行时的各项监控数据，分析系统主要的性能瓶颈并提出解决方案，对数据库进行调优，提供应用部署、系统变更和迁移等的现场支持服务，现场紧急救援及恢复，提交完整的巡检报告等。

服务内容

a、主机系统服务

针对数据库系统，技术服务内容包括：

①提供操作系统必要的升级与性能调优；

②操作系统的补丁安装；

③日志文件和空间整理、分析等；

④定期进行硬件系统维护；

⑤随时响应用户需求，完成数据库主机起、停工作；

⑥提供故障诊断和修复。

b、软件服务

软件服务内容包括：

①提供软件系统的安装、升级、迁移服务；

②根据现有环境对系统进行优化；

③对软件进行备份。

c、备份系统服务

备份系统服务内容包括：

①提供备份系统策略定义和调整；

②提供日志文件分析整理；

③提供故障诊断和修复。

④提供各应用备份需求，并进行备份实施。

d、存储系统服务

对存储系统提供日常巡检、故障处理、服务支持等服务。内容包括：

①提供存储系统策略定义和调整；

②提供日志文件分析整理；

③提供故障诊断和修复；

④提供存储空间调整等服务。

e、系统升级安装及测试服务

提供系统升级安装及测试服务，内容包括：

①对主机和存储OS版本升级计划提供建议；

②现场安装第三方软件；

③配置新版本操作系统，并恢复应用系统；

④测试新版本操作系统；

⑤对HA升级的计划及准备提供建议；

⑥配合将制定应用系统添加到存储中。

f、性能诊断与调试服务

对用户系统情况进行性能诊断，根据结果调整系统参数，是系统始终在最佳状态下运行。对可能出现的问题提供科学预测，并采用必要的预防和补救措施，防患于未然。具体如下：

①检查系统硬件使用情况；

②检查系统缓存使用的性能情况；

③检查磁盘I/O的性能情况；

④检查系统交换空间的使用情况；

⑤检查系统用于网络通讯的缓冲区使用情况；

⑥检查磁盘状态和使用情况。

**3.2.2安全设备**

1）巡检：专业技术人员上门对设备功能及应用环境进行全面的检测分析后给出后期设备稳定性及应用功能优化建议报告。

2）维护设备清单：详见设备清单《安全设备》

3）服务内容

a、URL&应用识别规则库升级：提供URL库与应用识别规则库升级有效期，保证产品能及时更新最新版本规则库

b、网关杀毒模块/网关杀毒升级许可：开通网关杀毒模块授权并具备更新有效期，保证产品能及时更新最新的病毒库

c、IPS漏洞防护+服务器防护功能模块授权/更新：开通IPS漏洞防护+服务器防护功能模块授权并具备更新有效期，保证产品能及时更新最新的漏洞特征库

d、实时漏洞分析模块/更新：开通实时漏洞检测分析模块并具备库更新有效期，保证产品能及时更新最新漏洞特征库

e、僵尸网络检测模块/更新：开通僵尸网络检测模块并具备库更新有效期，保证产品能及时更新最新漏洞特征库

f、网页防篡改模块：开通网页防篡改功能，保证我院网站内容不被篡改，避免因网站内容被篡改给组织单位造成的形象破坏、经济损失等问题

g、持续对基础功能和增强功能的安全能力进行升级，包括：AF、URL、WAF、IPS、等库的升级更新，保持设备具备检测防御最新威胁的能力

h、未知威胁防护与杀毒订阅服务:具备云端未知威胁检测功能，能及时识别0day攻击或病毒变种，然后立刻下发规则到本地防火墙，进行有效防御

i、增加防火墙VPN功能模块许可，数量20个，满足业务需求，包含IPsec vpn和ssl vpn

j、设备故障的排除，维修及备用机服务

**3.2.3网络设备**

网络、网络安全设备维护的目标是：通过网络、安全系统管理服务，降低网络设备故障率，提高网络设备的运行性能。提高网络运行的稳定性、可靠性，以专业化运作模式解决各类信息系统信息化发展的需求。需要提供故障诊断、远程支持、现场支持、软件升级、设备搬迁、网络优化、网络巡检、现场培训、技术交流、网络安全、网络建设建议等服务。

1）具体服务内容如下不限于：

a、网络故障排查

b、网络设备硬件状态检查

c、网络设备配置管理服务

d、网络设备资料整理，配置参数整理

e、网络使用状况趋势分析及建议

2）网络设备巡检流程如下不限于：

a、硬件检查

检查设备状态指示灯是否正常

检查设备电源模块是否有告警

检查设备组件是否完整

检查端口指示灯是否正常

检查设备繁忙度、分析。

系统功能检查

b、登陆设备

使用Web界面，连接管理地址即可登陆，或者也可使用XSHell等连接工具通过SSH、Telnet等方式进行登陆。以页面登陆为例：

查看界面是否有异常告警

系统健康度是否处于阀值状态

查看设备接口有无异常流量或者异常日志

如有异常情况及时记录并分析原因

**3.2.4机房基础环境设备**

●**空调、UPS、动环系统和配电系统维护**

主要包括机房精密空调、UPS、动环系统、配电系统硬件故障维护。具体巡检内容包括但不限于如下：

**1、精密空调**

设备的巡检，更换过滤棉、室外机清洗，故障排除及保养。

（1）控制系统：检查显示单元是否正常，各设置参数是否正确，查看历史报警记录对报警内容进行分析消除隐患。

（2）空气过滤器（室内外）：检查空气过滤器，如需更换则更换空气过滤器。

（3）加湿器：检查蒸汽加湿器是否结垢，如结垢需拆下加湿器进行清洗或更换。拆下蒸汽加湿器，检查三相加湿电极是否接触紧密，是否有破损，保证加湿时的电路安全。

运用维修模式检查上水是否通畅且速度平衡。

运用维修模式检查排水是否通畅。

运用维修模式检查三相加湿电流是否平衡，且在正常工作范围之内。

检查蒸汽输出口是否紧密、漏汽。

检查蒸汽输出量是否能够保证机房湿度。

（4）外部冷凝器：

检查冷凝器是否清洁，如需清洁需用专用的清洗工具清洗室外冷凝器。

风扇：检查风扇转动，有无异常噪声，运行电路是否正常。

检查室外冷凝器的电源开关，工作是否正常，绝缘是否可靠，电气接点是否紧固。

检查压力继电器，对室外风机的控制是否与设置的一致并且根据当时的具体工作环境调整压力断电器。

（5）蒸发器：检查蒸发器是否清洁，如有污垢用药剂清洗，保证足够的热交换量。

（6）室内外风机：检查风机马达运转是否正常，有无异常噪音，并且轴承是否发热，检查耗电量。对于由皮带传动的机组，检查传动皮带，用手指拉紧时，是否可延长2cm；

（7）电加热器：检查三级电加热器的各级加热电流及各电气接点是否正常。电加热器的过热保护是否灵敏。

（8）电路：

检查主电源及各支路的各相电压，电流是否正常。

检查所有的接触器，触点是否清洁，接触是否可靠、检测吸合的瞬间电流，对各接点进行紧固，确保安全。

对 24V 控制线路进行检测，确保控制的灵敏。

对各种的系统保护功能进行检测，（例如高压保护，低压保护，过热保护，相续保护等）保证设备的安全运转。

（9）制冷系统：

检查制冷系统运行压力（高压，低压）是否正常，并根据当时的室外环境对压力进行适当的调节。检查压缩机的三相绕组是否平衡，绕组的绝缘是否可靠。

进行过热度的测试，判断系统的运行效率是否能够达到指定的性能指标。

压缩机工作时的声音是否异常，以判定系统的润滑程度。

（10）排水系统：检查排水系统是否畅通，如有水垢或异物阻塞管道，用药剂疏通管道，保证排水顺畅。

**2、UPS系统**

维护内容：设备的巡检，故障排除及保养。

主要包括以下内容：

（1）监控面板

检测监控面板按键操作功能是否正常。

检测面板指示灯及蜂鸣器的功能是否正常。

检测 LCD 显示功能及其显示的日期时间是否正确，不准确的及时修正。

检查 UPS 系统及负载的运行数据，并进行评估。

检查当前存在的系统时件及历史记录，并进行评估。

检查电池、负载及市电的统计信息。

检查 UPS 显示参数与实际值较正。

（2）主机内部

UPS 机内清洁。

UPS 内部连接端子紧固检查及加固。

检查内部主要元器件（逆变器、整流器、静态开关等）。

检测主回路功率元器件。

主要控制板工作状态检查。

检测机器内部有无局部过热点。

（3）风机

运转平稳有无异常噪音。

风机温度正常有无故障报警。

（4）UPS 系统性能测试

系统常态模式工作是否正常。

系统旁路模式工作是否正常。

系统电池供电模式工作是否正常。

系统工作模式切换是否正常。

通信功能是否正常。

（5）UPS 历史记录的评估

记录重复出现的报警。

报警是否出现在每周、每天相同的时间。

报警是否与外电网有关系。

报警是否与负载有关系。

蓄电池组有关：

（1）环境检测项目

机房的清洁、温度、空调通风等环境状况检测。

蓄电池的表面温度。

设备四周及上面是否有堆积物。

电源布线、金属柜、家接地线、各接线端子连接检测。

（2）物理性检查项目

检查极性、连接条是否清洁，有否氧化或腐蚀现象。

检查连接处有无松动及电池绝缘情况。

检查蓄电池极柱有否爬酸、漏液，安全阀周围是否有酸液溢出。

检查蓄电池壳体有无损伤，渗漏和变形，极柱有无损伤、变形。

检查蓄电池及连接处温升有无异常。

**3、动环系统**

维护内容：设备的巡检，故障排除及保养。

检查动环主机运行状态

检查室内摄像头是否正常录像

检查室内温度传感器是否正常

检查室湿度传感器是否正常

检查室内红外传感器是否正常

检查室内漏水传感器是否正常

**4、配电系统**

维护内容：设备的巡检，故障排除及保。

（1）检查屏幕显示各项电压、电流等各项参数是否正常。

（2）检查电缆接头有无发热变色，接地线有无锈蚀，有锈蚀的及时做防腐处理。

（3）检查电容柜内的电容器外壳是否良好，有无渗漏，膨胀情况，指示灯是否良好，对异常的电容器及时更换。

（4）检查各电容器外壳接地线接触情况。

（5）每月做好各柜体的保洁除尘工作。

（6）检查二次回路接线是否牢固，熔断器是否完好以及绝缘电阻的摇测。

（7）电容柜的检查：断开空气开关不带电容器时对电容控制器进行动作试验，应先合的先断，后合的后断，应正常。对过压保护，欠流保护，投切门限值进行调整。

（8）检查各指示灯应完好，对断路器，漏电断路器，热继电器，时间继电器等进行检查。

（9）检查各柜体控制器开关位置是否正常，运行应正常，手动调试机械连锁部分合闸是否可靠。

**3.3病房呼叫系统**

病房呼叫系统是指医院内病人与护士站护士沟通的交互系统，由床头分机、门口分机、护士站主机、综合布线等部分组成，我院现有病房呼叫系统采用南格呼叫系统，由于系统是由电子设备组成，病人使用频繁，配件容易损坏，一旦损坏影响病人呼叫护士诊疗，所以需要将配件备到医院便于及时更换，按照备件列表要求提供。供应商需提供原厂服务，并提供证明文件

1）备件列表：

|  |  |  |  |
| --- | --- | --- | --- |
| 序号 | 备件名称 | 数量 | 备注 |
| 1 | 护士站主机 | 2 | 要求与原系统兼容，需提供兼容性证明 |
| 2 | 床头分机 | 10 | 要求与原系统兼容，需提供兼容性证明 |
| 3 | 床头分机呼叫绳 | 20 | 要求与原系统兼容，需提供兼容性证明 |
| 4 | 门口分机 | 2 | 要求与原系统兼容，需提供兼容性证明 |
| 5 | 主机听筒 | 10 | 要求与原系统兼容，需提供兼容性证明 |
| 6 | 主机听筒绳 | 20 | 要求与原系统兼容，需提供兼容性证明 |
| 7 | 呼叫器专用8口交换机 | 4 | 要求与原系统兼容，需提供兼容性证明 |
| 8 | 分机通讯模块 | 20 | 要求与原系统兼容，需提供兼容性证明 |
| 9 | 串口线 | 5 | 管理电脑与护士站主机通讯 |

2）病房护理呼叫系统维护范围包含外科大楼病区、内科大楼病区、创伤中心病区。

3）服务内容：

包含我院所有病区医护护理呼叫系统的所有设备（主要包括护士站主机、床头分机、床头分机呼叫绳、门口分机、主机听筒、主机听筒绳、呼叫器专用8口交换机、分机通讯模块、串口线、卫生间分机、系统电源、走廊显示屏等）。服务内容：备件采购、故障排除及维护、返厂维修、定期巡检等。

**3.4等保评测**

|  |  |  |
| --- | --- | --- |
| 评测项目 | 医院网站系统  医院综合管理平台  HRP系统 | |
| 工作内容及要求 | 定级备案 | 提供对信息系统的定级备案技术咨询服务，协助完成信息系统定级备案工作。 |
| 等级测评 | 严格按照等级保护2.0相关技术规范，对现场测评结果分析、汇总后形成被测信息系统的等级测评报告，说明信息系统存在的安全问题及提出相应的整改建议，为信息系统进行等级化建设、安全整改、等级保护建设验收提供依据。 |
| 渗透测试 | 提供渗透测评服务，通过工具扫描、人工渗透验证等方式，发现系统漏洞及隐患，形成被测系统渗透测试报告。 |
| 整改咨询 | 结合该测评项目的实际情况分析信息系统安全情况与等级保护基本要求的差距,从技术和管理两个方面编写整改建议报告。 |
| 配合验收 | 整理项目过程中所有相关的过程文档，提交甲方相关人员。 |
| 售后服务 | 为期一年的售后服务工作中，服务方将向延安市中医医院提供包括应急响应、安全监测、配合检查、电话支持、安全咨询等服务在内的安全维保服务。具体服务内容如下：  （1）应急响应服务  针对本次项目，服务方提供7X24的常规应急响应及灾难恢复专家服务。在接到用户故障报修电话10分钟内响应。对客户信息网络应用系统突发的信息安全事件进行响应、处理、恢复、取证、跟踪、事后分析的方法及过程。  （2）配合检查服务  服务方免费协助延安市中医医院响应公安机关、单位内部以及第三方机构针对信息系统安全等级保护工作的检查工作。服务内容包括协助延安市中医医院准备、完善各类资料文档，配合检查过程中的答疑及技术支持及其他现场检查的响应。  （3）电话支持服务  每周7天/每天24小时不间断的电话支持服务，解答延安市中医医院在使用过程中遇到的问题，及时提出解决问题的建议和操作方法。电话响应时间不超过10分钟，到达现场时间不超过2小时，解决问题不超过24小时。  （4）安全咨询服务  服务方为延安市中医医院免费提供一年技术咨询服务，包括信息系统整改建设咨询服务以及其他相关安全咨询服务，一旦接到用户的服务请求，技术服务工程师将立即开始提供服务，帮助客户解决信息安全相关技术问题，全面配合延安市中医医院做好业务系统全保障工作。 | |
| 交付物 | 《信息系统安全等级保护定级备案证明》  《信息系统安全等级测评报告》  《信息系统整改建议书》  《信息系统渗透测试报告》 | |

**3.5杀毒软件升级**

\*总体要求：延续医院终端数量使用（1000点位）授权一年，新增服务器端杀毒软件授权50点位；与医院HIS、LIS、PACS、移动护理等应用系统实现兼容，需提供与医院相关主要应用系统的兼容性证明。终端提供主动式病毒防御、攻击保护、木马检测、漏洞修复、外设管控、网络管控及软件管理等功能，同时提供系统优化、垃圾清理及运维工具等辅助功能。有效防范来自移动设备、漏洞传播、网络共享、邮件、网页、网络下载等各种途径的病毒入侵，实现全方位的病毒防护。

技术要求：

1、产品架构: 要求产品可以软件+硬件形式交付，包含管提控制中心、客户端软件及其它辅助硬件

2、基本功能：产品全功能支持简体中文/繁体中体/英语自由切换。支持终端用户和管理员是一套账号管理系统，简化账号管理复杂度，一个账号解决所有身份认证，既可以用于终端登录，也可以用于管理管理中心。支持自动分组，按IP地址、CPU数量、MEM容量、主机名、计算机工作组等参数进行自动动态调整分组。管理控制中心当登录账号输入密码错误次数超过锁定阈值后账号将被锁定，且可设置锁定时间，该时间内账号登录请求不被接受。同时应支持双因子认证登录方式，提高安全性。支持在线更新病毒库、补丁库、威胁情报等数据，并且支持“按月、按周、按天、按小时”灵活设置更新时间。支持隔离网环境更新数据。

3、病毒防护：病毒扫描支持扫描所有文件和仅扫描程序及文档文件设置，支持对压缩包文件设置最大扫描层数和大小，当发现压缩包内存在病毒时，还需继续扫描压缩包内其他文件。支持对压缩包内的病毒扫描，支持多层压缩包的扫描，可自定义配置压缩包的扫描层数，至少大约10层模式下的扫描。支持对进程防护、注册表防护、驱动防护、U盘安全防护、邮件防护、下载防护、IM防护、局域网文件防护、网页安全防护、勒索软件防护。支持自动阻止远程登录行为，防护黑客远程爆破和拦截恶意的远程登录。支持僵尸网络攻击防护，对流出本机的网络包数据和行为进行检测，根据策略在网络层拦截后门攻击、C2连接等威胁。支持不少于三个杀毒引擎混合使用，提高病毒检出率。

4、补丁管理：支持对Windows操作系统、IE、.NET Framework、Office、Adobe Flash Player、Adobe Acrobat和Adobe Acrobat Reader DC、硬件驱动更新等软件进行补丁修复。支持管理员预先设置好灰度发布批次和漏洞修复策略（分时间段、按级别、排除有兼容性问题的补丁等），每当控制台更新补丁库，自动化编排完成漏洞修复——将全网终端划分为由小到大的多个批次，根据企业环境，自动先推送给第一个小批次分组，如无问题自动推送给下一个批次，直到推送给全网。如有问题，只需将有问题的补丁添加到排除列表和卸载已安装的终端即可。整个推送安装过程自动化编排，无需管理员过多参与，只需在有问题时添加排除列表和下发卸载补丁任务。补丁语言种类需支持中文，繁体中文，英文。允许终端用户手动修复漏洞，如果发现“修复内容”中设置的需要修复的漏洞和功能缺陷没有修复成功则提醒终端用户修复。支持按照补丁的维度统计补丁安装情况，包括补丁号、系统类型、补丁类型、补丁级别、补丁名称、补丁描述、发布日期、漏洞CVE编号、漏洞CNNVD编号、未安装、已安装、已安装未生效、已排除、未更新补丁库。并支持导出统计报表。

5、终端管理：支持外设库管理，可统计终端外接的各种设备，包括厂商和设备类型、产品、数量、PID、VID和设备来源。）支持对支持对外设进行多维度的放行，包括设备名称、PID/VID、实例路径，通过添加实现例外或加黑。（提供产品界面截图）支持终端进程红名单、黑名单、白名单功能。可设置核心进程必须运行，也可保护核心进程不被结束，违规并告警。支持统计终端的出口地址列表，搜集终端连接的无线信号信息统一展示，标识出ssid可连通互联网，可连通服务器的情况，汇总展示内网终端上报的进程信息，支持设置进程匹配规则，其它业务可直接调用创建好的进程规则或者进程分组。支持对终端节能管理，支持对长时间运行、定时关机、空闲节能、工作时间外开机等节能类型设定策略，支持仅提示、关机、注销、锁定、关闭显示器、锁定+关闭显示器、休眠和睡眠处理。并支持提示倒计时弹窗，可设置在终端取消后下一次提醒时间。支持对网卡进行防护，支持阻止终端修改IP地址、使用动态IP地址、热点创建和IPV6地址使用等，可自定义提示内容和生效时间。

6、\*售后服务：一年维保服务，一年病毒、补丁库、规则库升级服务，提供原厂项目授权及一年售后服务承诺函原件

**3.6网络安全运营服务**

资产梳理：

1）通过搜索引擎及网络爬虫等多种技术相结合，通过对关键字、域名及IP的综合查询及关联分析，从而为客户梳理出互联网资产全景图的服务。客户根据互联网资产的分析和评估，相关业务部门可及时对发现的安全风险进行修复，消除安全隐患。

2）通过资产识别工具结合人工核查方式对内网信息系统主机资产和Web服务进行全面深入的梳理，实现内网资产台账的全生命周期的动态管理，提升内网资产台账梳理的工作效率。

基础安全评估：

安全工程师通过对网络和主机的扫描，了解网络的安全设置和运行的应用服务，及时发现安全漏洞，客观评估网络风险等级。根据扫描的结果更正网络安全漏洞和系统中的错误设置，有效避免黑客攻击，做到防患于未然，最终输出《网络安全检查报告》。

3）漏洞处置服务：

基础安全评估过程中针对疑似被攻陷系统和高危漏洞，经评定与甲方负责人协商后（对于无法修复的漏洞、更新漏洞后可能造成业务无法正常运行、官方未发布漏洞补丁等情况，通过甲方现有安全设备进行配置策略的优化），通过专用分析工具与人工结合的方式进行处置。

### 3.7易损件备用服务

易损件备用服务：投标人需提供一定金额的备用金用于易损件备用服务，备用金总额为成交价的8%（不包含病房呼叫系统配件），具体使用办法以最终合同为准。

**3.8运维服务方式**

驻场人员，每日巡检机房、填写运维记录，提供定期现场巡检故障处理的服务，定期巡检服务包含但不限于：

**3.8.1常规巡检**

**（1）月度巡检服务**

每月对各系统及设备进行检查，进行个系统检查，进行漏洞扫描，并对检查中存在的故障及安全隐患进行处理。每月第一周向用户单位提交上月的《月度巡检报告》，报请用户单位审批签署。

工作月报汇报内容包含：上个月主要工作完成情况，包含日常运维、定期巡检、重点工作，未完成工作情况；本月重点完成工作；

提供运行报告：系统运行报告反映当前各个系统状态，主要包括：各系统运行状态监测分析，存在问题，解决方案，一般情况下，在次月5日前提交上月运行报告

提供故障报告：针对各个系统发生的事故和故障，编写故障报告。一般情况下，在事故处理完成后的两天之内提交故障报告

定期完成信息安全管理抽检，及时发现信息系统安全管理落实及安全技术实施中存在的不足及风险，检查内容包括但不限于：安全管理制度及执行情况、防病毒系统版本升级情况、终端用户的安全合规情况、安全设备的系统性能情况、系统开放服务及安全策略检查等，并提出安全检查报告，对检查中发现的安全问题或缺陷，给出合理的安全整改建议

**（2）季度巡检服务**

每季度对由维护团队的专业维护队伍对所有设备进行安全评估和风险分析，提交完整的安全状况评估报告，分析存在的安全漏洞情况，提出《整改方案和建议》。

**（3）年度巡检服务**

每年由维护团队组织相关的专家（含硬件和软件）对整个系统进行安全检查，对每个硬件设备使用状态进行风险评估，并对下一年可能存在的问题进行风险预测，并出具年度服务报告。

**（4）现场故障处理服务**

提供至少一名驻场工程师，服从甲方管理，在维护期内提供5\*8小时的驻场服务，提供7×24小时故障响应服务。

**（5）临时保障服务**

当遇到重大活动需要提供临时保障服务时，需在进行保障服务的提出服务需求，对服务进行评估后安排相应数量的工程师提前2天入驻用户现场，并对所有设备进行临时性安全检查，排除安全隐患，以做到万无一失。

**（6）应急响应服务**

1、提供应急演练服务一次，包括应急预案修订，协助开展应急演练。帮助医院建立安全应急机制，完善应急措施、建立专项应急预案，定期组织培训，每年开展至少一次有针对性的应急演练活动。

2、提供应急响应服务于重大活动安全值守，应针对信息系统制定应急响应快速服务流程，一般时间4小时响应服务，确保系统安全稳定运行。

3、提供设备故障处置服务，在设备出现故障时，现场人员应能够及时对故障情况进行检查、判断，采取应急措施保障业务正常运行，并协助客户快速解决设备故障问题。

**3.8.2服务方式**

人员要求：至少1名驻场服务人员，主要系统设备出现故障时，5分钟内响应，半小时内专业工程师赶赴现场进行故障诊断及处理。工程师到场后，在1小时内排除普通故障，2小时内排除较大故障，4小时内排除重大故障，12小时内排除特大故障。

时间要求：5\*8小时驻场服务，7\*24小时电话响应。

1、热线电话服务：指派有丰富经验的工程师提供7\*24小时电话服务，以便提供紧急支持，随时免费解答技术问题；

2、现场服务：提供现场服务，解决服务范围内软硬件设备存在的问题。

3、远程诊断：提供远程服务（如拨号、远程控制等方式）对设备进行诊断和修复。

4、定期巡检：派经验丰富的工程师到现场对服务范围软硬件设备内进行定期巡检，每次巡检需检查服务范围内所有内容，服务报告需双方签字确认。

**四、服务规范及要求**

4.1服务项目管理规范（10分）

维护团队派遣具有专业知识的资深管理人员负责本项目的项目管理，根据我院的实际情况制定巡检、配件更换等流程及内容，统筹相关工作，项目监督与情况汇报，控制工作质量和预算，执行变更和应急情况管理，并根据实际状况调整服务方人员安排，以保证此项目的正常高效运作。

每月考核得分。

4.2服务质量管理规范（15分）

维护团队根据本项目要求提出服务质量管理及监控具体措施，并对所提供的服务质量和标准做出明确可量化的承诺。

每月考核得分。

4.3 服务响应时间规范（25分）

各级故障事件的最晚响应时间为：

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 确认时间 | 一级故障事件 | 二级故障事件 | 三级故障事件 | 四级故障事件 |
| 1小时 | 技术服务人员 |  |  |  |
| 4小时 | 专业工程师 | 技术服务人员 |  |  |
| 8小时 | 技术支持专家 | 专业工程师 | 技术服务人员 |  |
| 12小时 | 服务项目经理 | 服务项目经理 | 专业工程师 | 技术服务人员 |

故障事件等级划分如下：

一级故障事件：现有的网络或系统停机，或遭到严重攻击行为或安全事件，对信息系统的业务运作有重大影响；

二级故障事件：现有网络或系统的操作性能严重降级，或由于网络性能失常或安全事件严重影响信息系统用户业务运作；

三级故障事件：网络或系统的操作性能受损，安全事件（例如病毒在小范围内发作），但大部分业务运作仍可正常工作；

四级故障事件：在网络、服务器、存储、安全设备功能、安装或配置方面需要调整或优化。本级故障事件对信息系统的业务运作几乎无影响，或影响很小。

依据事故重要性和紧急性的原则，每一级事故严格定义升级时间为2小时，其中在二级事故和一级事故应急处理过程中，要及时考虑替代恢复方案，尽可能在最短的时间内恢复业务系统。其中三级事故的处理，驻场服务人员在事故响应1个小时内，如果不能快速判断问题所在，可以寻求整个服务团队的支持。在一、二级事故判断中，服务人员在监控中发现问题，一方面应迅速将问题向部门领导进行反应，一方面须快速判断问题和收集事故信息，涉及到具体产品提供商或服务商内，及时协调相关厂商现场支持。为保障业务平台的正常运行，除对突发故障的应急支持外，要充分保障日常对业务系统软硬件的应急灾备恢复预案，并通过定期的演练加强应对突发事故的意识和流程。

每月考核得分。

4.4现场服务支持规范（25分）

运维服务人员要做到耐心、细心、热心的服务。工作要做到事事有记录、事事有反馈、重大问题及时汇报。严格遵守工作作息时间，严格按照服务工作流程操作。

★供应商需具备运维资质，并提供ITSS运维管理体系认证证书

★派遣至少一名一线驻场人员，工作日入驻机房现场服务；一线驻场人员需具备服务内容方向至少一项认证证书。一线驻场人员负责日常巡检、故障处理及服务需求响应，重要且不常发生的事务由后台的资深技术团队定期或不定期地同驻场人员一起完成。

★二线支持：不需驻场，组建不少于15人的二线团队，需具备服务方向专家能力，根据需要提供定期或不定期的技术支持。二线团队应由多个技术领域的资深技术专家组成，领域包含：项目管理、服务器、存储、网络、操作系统、数据库、备份、机房环境等。从技术能力和经验上讲，二线资深技术专家要强于驻场人员，加之以多名资深专家组成团队的形式提供服务，整体技术能力更为强大。对现场特定的事务进行有针对性的支持，和一线人员的工作互补，以实现整体运维服务的价值。

现场支持工程师应着装整洁、言行礼貌大方，技术专业，操作熟练、严谨、规范；现场支持时必须遵守用户单位的相关规章制度。现场支持工程师在进行现场支持工作时必须在保证数据和系统安全的前提下开展工作。现场支持时出现暂时无法解决的故障或其他新的故障时，应告知用户并及时上报负责人，寻找其他解决途径。故障解决后，现场支持工程师要详细记录问题的发生时间、地点、提出人和问题描述，并形成书面文档，必要时应向用户介绍故障出现的原因及预防方法和解决技巧。

每月考核得分。

4.5服务行为规范（15分）

遵守用户的各项规章制度，严格按照用户相应的规章制度办事。

与用户运行维护体系其他部门和环节协同工作，密切配合，共同开展技术支持工作。

出现疑难技术、业务问题和重大紧急情况时，及时向负责人报告。

现场技术支持时要精神饱满，穿着得体，谈吐文明，举止庄重。接听电话时要文明礼貌，语言清晰明了，语气和善。

遵守保密原则。对被支持单位的网络、主机、系统软件、应用软件等的密码、核心参数、业务数据等有保密责任，不得随意复制和传播、签订保密协议。

4.6服务报告规范（10分）

维护团队定期提供服务报告，服务期结束前应提供服务年报，并对每一次重大故障和问题的原因、解决方法、完成情况等形成专门报告，及时报送医院。在运维服务过程中将产生不限于以下的记录和报告：

系统巡检日志

系统维护记录

故障分析处理记录

故障整改方案和建议

重大故障记录报告

后期规划建议

**五、交付物**

（1）设备台账统计表（包含设备信息、设备连接链路信息）

（2）设备网络拓扑图和连接拓扑图

（3）设备日常维护手册

（4）每季度巡检报告

（5）各系统巡检报告

（6）培训记录

（7）提供应急演练方案及记录