## **江苏省第二中医院中心机房运维项目调研需求**

****一、项目基本情况****

江苏省第二中医院中心机房运维项目

调研需求：

此次维保范围为江苏省第二中医院的1个中心机房（核心区域），以及1个辅助机房（UPS控制机房及UPS电池室）和楼宇弱点机房24个。机房内共有业务硬件设备（含网络、安全、服务器、存储、工控等）100余台设备在运行。维保共有以下几项基本需求：

1、提供2人以上驻场服务，完成日常机房巡检、业务硬件设备的基本维修保养、网络、安全、业务系统的基本调试以及其他院方交办的各类与中心机房业务相关的工作（工程师需了解各类主流机房信息化设备，能够熟练使用操作各类设备，如网络设备命令配置、虚拟化资源调配等）；

2、高级工程师定期巡检：由公司组件高级技术工程师团队，针对医院各类设备及网络环境的健康进行定向巡检，分析和协助解决医院各类存在的安全隐患（1季度1次）；

3、二线技术专家团队支撑：提供7\*24小时的服务保障，灵活应对各类突发事件，有效预防和最大程度地降低系统各类突发事件的危害和影响，保障信息系统安全、稳定运行；

4、配套资产及运维管理软件，针对医院中心机房资产实现数字化梳理、可视化管理医院机房各类设备，日常运维工作形成工单以及知识库，便于后期的管理和学习；

5、机房业务硬件设备维保：针对于主要脱保但在用的业务服务器、存储等设备的故障维修、配件更换；

6、主干核心重要设备的备件保障：主要针对中心机房单节点核心或主干重要设备（如服务器、存储、防火墙、交换机等）提供备件支撑服务。以便设备故障导致业务受到影响后能及时恢复。所提供的备品备件能够与原设备兼容使用，把设备突发故障所造成的停工损失减少到最低限度（备件使用后返还）。

7、网络安全专项值守服务保障：自备安全运维工具和设备，结合医院现有安全设备，针对院内网络安全情况进行7\*24小时实时监测，并通过微信、电话、邮件等多种方式提供实时安全提醒，协助处理各类安全事件；根据院方需要，定期针对院方业务系统进行无感知安全扫描，检查安全漏洞，协助整改；针对核心业务服务，提供渗透测试服务，深度挖掘安全漏洞；配备攻防演练平台，提供攻防演练服务，组织攻防提升综合防护能力；提供安全服务平台，可视化展示各类周期性安全报告、事件及其闭环处理流程记录等。