# 杏林感染实时监控系统

# 运维服务参数

一、服务内容

1.在维护期内，需提供系统软件产品的故障排除服务，保证用户的正常运行使用，针对系统出现的故障，提供专业的排查和修复服务，快速定位问题根源，采取合适的解决方案，确保系统能稳定运行，故障处理后不会反复出现。不得违反实时政策要求、院内管理规定等。针对一些独特的、不可预知的、客户自身不能处理的突发事故，需提供上门服务，若突发事故由硬件或第三方因素造成，相关费用由客户承担，具体金额双方自由协商。若因本软件自身功能缺陷不能正常运行，提供免费技术支持和服务。

2.提供符合院方要求的安全机制确保本系统及所连接的系统的数据安全，保证数据不被非法利用和盗用。

3.针对服务期间修改/升级的软件功能提供培训服务，需对院感专职人员进行培训，使其能很好的掌握监控系统的功能。

4.应定期监控服务器的各项指标，及时发现运行异常、性能下降等问题，并及时预警和报警，确保系统能及时应对各种异常情况，当服务器硬件资源不足或硬件出现故障是应及时联系探讨解决方案。

5.定期进行系统性能测试和调优，包括检查系统资源利用率、系统响应时间、内存使用情况等，针对系统进行优化，提高系统性能和效率，避免因性能问题而影响用户体验，确保系统性能稳定和高效运行。应掌握windows、Linux、centos等系统，可根据需求对数据库及中间件维护、高可用、负载均衡等建设。

6.根据需求和实际情况对系统进行调整和变更，保障系统的稳定运行及数据的准确性。包括现有报表格式、数据调整、修改；从系统现有数据中新增报表单。对应用软件存在的潜在性错误进行免费修改，该修改以版本升级形式完成。软件应用过程中出现功能错误时，协助查找、排除软件故障，保证系统功能正常运行。应用模块范围内的功能需求调整、修改。如遇到与其他系统对接或对外提供数据接口时应予以配合。

7.应建立系统备份和恢复方案，包括完整备份、增量备份等方式等，并提供恢复服务，确保系统出现异常情况时能够及时恢复正常运行，并定期做数据验证恢复测试，确保备份数据的完整性和正确性。

8.应及时对系统进行安全加固，漏洞扫描和修复定期更新漏洞库、软件补丁管理，以及紧急漏洞事件的应急响应、加强系统安全防护等。

9.应提供接口文档、系统表结构等相关文档，并在调取数据时提供帮助。

10.对维护过程中涉及到的所有数据、信息进行严格保密，不得泄露。

1. 维护服务要求

1.服务渠道及响应时间

如果本产品发生故障，乙方为用户提供电话、远程、现场协助等技术支持，电话响应时间不超过1小时，到现场时间不超过48小时。

2.现场巡检服务

应至少每年2次现场对系统进行现场巡检和检查，确保系统按照规范运行，同时及时发现潜在的风险，避免系统出现严重问题。包括硬件和软件状况、备份情况、安全性等。到现场检查系统模块运行情况，与维护人员沟通，提供常见问题的解决办法，巡检结束后提供巡检报告。

3.培训要求

乙方根据甲方要求为甲方培训管理人员提供培训，使部分问题可以由客户技术人员在第一时间得到解决。包括功能配置、字典维护、参数调整等正常的维护工作。

4.系统灾难发生时，乙方承诺立即响应，减少数据损失，降低灾难对整个系统正常运行的影响。

5.文档支持

协助提供甲方所需要产品、项目实施等有关文档，不涉及产品知识产权及商业机密的文档资料。

6. 服务期内配合甲方定期开展网络安全自查，自查内容至少包括系统日常运行情况、系统漏洞等；配合甲方定期进行安全审计，审计内容至少包括系统账号、权限、操作行为和安全技术措施有效性等，及时发现和处理信息系统运行过程中的安全隐患，减少或避免网络安全事件的发生。