# **反统方数据库审计系统维保需求**

## **一、维保范围**

本次反统方数据库审计系统维保服务，包含软件系统的所有功能模块、中间件以及与之相关的接口程序等。及硬件设备维护，确保整个软件生态系统的稳定运行。

## **二、服务内容**

1. ****故障诊断与修复****：在系统出现故障或异常时，维保团队需在接到故障通知后 2小时内响应，通过远程或现场方式，快速定位故障根源，并进行修复。修复完成后，需进行全面测试，确保软件恢复正常运行且无衍生问题。
2. ****性能优化****：每季度对硬件和软件系统进行巡检，分析系统在运行过程中的资源占用、响应时间、吞吐量等指标，针对发现的性能瓶颈进行优化。确保软件在高并发、大数据量等复杂场景下仍能保持高效稳定运行。
3. ****安全维护****：建立完善的安全防护体系，一旦发生安全事件，需立即启动应急响应机制，在4小时内采取有效措施进行处理，并向用户提供详细的安全事件报告。
4. ****数据管理****：制定数据备份与恢复策略，定期对软件系统的数据进行全量或增量备份，确保数据的完整性和可用性。备份数据需存储在安全可靠的存储介质中，并定期进行恢复测试，以验证备份数据的有效性。在数据丢失或损坏的情况下，能够在规定时间内完成数据恢复工作。
5. ****功能完善与升级****：根据用户提出的合理需求以及市场技术发展趋势，对软件进行功能完善和版本升级。在升级前，需进行充分的测试和评估，制定详细的升级方案和回滚预案，确保升级过程平稳，不影响软件的正常使用。升级完成后，需对用户进行培训和技术支持，帮助用户熟悉新功能和操作流程。

## **三、服务方式**

1. ****远程支持****：通过电话、邮件、即时通讯工具、远程桌面等方式，为用户提供 7×24 小时的远程技术支持服务。用户在遇到问题时，可随时联系维保团队，获取及时的技术指导和解决方案。
2. ****现场服务****：对于远程无法解决的复杂问题或紧急故障，维保团队需在8小时内派遣专业技术人员到达现场进行处理。现场服务人员需具备丰富的技术经验和良好的沟通能力，确保问题得到快速、有效的解决。
3. ****定期巡检****：维保团队需每季度对软件系统进行现场巡检，检查系统的运行状态、硬件设备情况、软件配置等，及时发现潜在问题并进行处理。巡检结束后，需向用户提交详细的巡检报告，包括系统运行情况分析、问题处理建议等。

## **四、服务标准**

1. ****响应时间****：对于紧急故障（如软件系统完全瘫痪、数据丢失等），维保团队需在 2小时内响应，并在8小时内解决问题；对于一般故障（如部分功能异常、性能下降等），需在 2小时内响应，并在3个工作日内解决问题。
2. ****服务质量****：维保团队需确保软件系统的可用性达到 95% 以上。
3. ****技术支持****：维保团队需配备足够数量的专业技术人员，技术人员需具备相关的专业资质和丰富的项目经验，定期参加技术培训和学习，不断提升技术水平。

## **五、其他要求**

1. ****维保期限****：本次软件维保服务期限为 1年，自合同签订之日起计算。在维保期限内，维保团队需按照本需求文档的要求，为用户提供全面、优质的软件维保服务。
2. ****保密条款****：维保团队需严格遵守用户的保密要求，对在软件维保过程中接触到的用户数据、商业机密等信息进行保密，不得向任何第三方泄露。在合同终止后，仍需继续履行保密义务。

 信息中心