# 用户需求书

## 项目背景

广东南方新媒体股份有限公司在2019年建设了一套IPTV用户行为分析系统，由神策网络科技（北京）有限公司进行建设，现计划对该套系统采购维保服务。

## 维保系统清单

|  |  |  |
| --- | --- | --- |
| **系统名称** | **服务描述** | **维保服务期** |
| 用户行为分析系统 | 提供系统软件的维保服务，保障系统的稳定、高效运行，包括但不限于应用系统、相关组件及保证应用系统正常可用的周边配置服务，例如除服务器硬件设备以外的操作系统、网络配置、中间件和应用软件的整体运维保障 | 合同签订起1年 |

## 服务要求

### 1.1维保服务要求

提供7×24服务响应级别。

(1)服务时间：7×24小时。

(2)响应时间：要求中标人即时响应，并在接到报修后30分钟内向采购人提出故障处理方案。

(3)到场时间：要求中标人在规定时间内远程接入提供维护服务，如需要到现场，中标人需在规定时间内到达采购人指定现场提供维护服务。

(4)故障恢复时间：要求中标人在规定时间内恢复故障，并在故障恢复后1个工作日内提供故障报告。

(5)响应时间及服务响应时间

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **故障级别** | **故障级别说明** | **电话响应时间** | **远程接入响应时间** | **现场响应时间** | **恢复系统正常运行时间** |
| 严重 | 影响业务系统全部或部分交易故障 | 10分钟 | 15分钟 | 3小时 | 2小时恢复系统正常运行 |
| 重要 | 业务系统全部或部分交易运行缓慢 | 10分钟 | 20分钟 | 6小时 | 5小时恢复系统正常运行 |
| 一般 | 一般报警信息，对交易系统正常运行没有影响；系统参数调整等 | 10分钟 | 30小时 | 12小时 | 24小时恢复系统正常运行 |

### 1.2软件更新服务

提供软件BUG的定位和修复服务，发现产品中疑似BUG，向中标人进行反馈，中标人根据采购人的反馈现象进行测试验证，如果是产品BUG，中标人排期进行软件BUG修复，发布版本之后，对采购人的系统进行修复，包括但不限于产品自身软件BUG、产品所依赖的操作系统、中间件、数据库等各组件所发现的漏洞修复。

### 1.3运维保障服务

提供7\*24小时应急响应及保障服务，保证系统的稳定可靠运行，包括电话、远程、现场方式。

1.3.1提供7\*24小时应急响应及保障服务，确保系统稳定可靠运行；

1.3.2提供现场升级、维护服务；

1.3.3运维保障服务包括但不限于应用系统、相关组件及保证应用系统正常可用的周边配置服务，例如除服务器硬件设备以外的操作系统、网络配置、中间件和应用软件的整体运维保障；

### 1.4系统巡检服务

对采购人环境进行全面诊断、巡检，发现存在的问题或风险点，并对存在的问题进行整改。

1.4.1包含系统资源使用分析、原系统产品组件检查、大数据组件检查、数据导入检查等服务内容，服务范围包含：系统整体健康状态检查、指出存在的风险和隐患，及建议的处理方式，包括问题处理、风险规避及相关优化服务。

1.4.2提供巡检和现场重点保障（春节两会、国庆两个重保期前的巡检）。

1.4.3每年不超过一次临时特殊保障期的巡检检查和重点保障。

### 1.5产品技术支持服务

提供7\*24小时产品技术支持服务，包括电话、远程、现场方式，提供产品使用、产品异常问题诊断等服务。

1.5.1产品使用答疑：提供产品使用方面的咨询答疑和基于产品功能的逻辑答疑；

1.5.2异常诊断

1）数据差异性诊断：包括原系统自身业务系统内数据差异，给出统计口径的分析和答复；

2）产品提示异常或者访问异常诊断：根据产品提示的异常，诊断出异常的原因，并告知方法；

3）系统性能的问题诊断：分析系统使用现状，诊断出现有系统使用的瓶颈，提供建议。

### 1.6业务扩容、迁移及割接

协助采购人完成迁移前的评估、新环境资源评估、新环境部署、系统扩容、老环境版本升级、实施迁移、迁移后的验证、迁移后的注意事项通知、数据导入、数据导出等工作。

### 1.7业务验证及应急演练服务

若采购人的环境进行调整，如网络调整、机房调整、上下游等环境进行调整，需配合采购人进行调整以及系统运行状态确认和业务验证；

为保证系统的可靠运行，检验应急响应中协同反应水平和实战能力、评估应急响应预案的实用性、可行性、可靠性，依据应急预案，需对系统进行可靠性、应急演练，需提供演练方案和安排安全人员进行演练，并做好总结和问题修复。

### 1.8信息安全服务

系统平台需符合相关安全规范要求，包含与系统平台相关的组件的漏洞修复和安全策略加固。每年配合采购人完成等保的测评，对等保测评、渗透、扫描及相关安全检查等发现的安全问题、公布的安全漏洞等进行整改及安全策略加固，包含不限于操作系统、中间件、应用软件等层面漏洞修复和安全策略加固。