附件：

**中心机房运维管理和电子设备维修保养**

**服务外包项目需求**

一、维保项目概述

为了保障和提高中心的IT服务质量，解决当前中心运维管理工作服务方面日益增长的需求和有限的提供能力之间的矛盾，计划将电子信息、机房基础设施等维护工作进行外包，由专业IT公司安排技术服务工程师进行驻场服务，提高中心的软、硬件的运行维护效率，确保各类信息系统正常运行。

二、维保服务工作范围

（一）负责中心计算机机房（数据中心机房、备份机房、视频机房）定期维护、巡检及故障处理工作，确保中心整个网络信息系统基础设施的正常运行。按照业主实际工作需求，提供上门的现场巡检、维修调试、故障恢复、操作系统的安装、现场培训等服务，及时发现并协调相关技术团队处置存在问题，确保中心机房内部的所有支持网络信息系统正常运转的关键信息基础设施，包含有消防、电力、空调、环境等，全年安全、持续、稳定的提供服务。

（二）负责我中心的现有的电子设备（台式电脑、笔记本电脑、打印机、扫描仪等等，详见中心电子信息类设备清单）维修保养具体工作实施，安排专业技术人员驻场开展设备日常维保工作，及时处理中心各科所提交的设备维修申请，修复设备或者网络故障，提高维保工作效率，确保中心职工的电子信息设备正常使用。

三、维保服务工作周期

维保服务工作周期为自签订合同之日起壹年。

四、维保服务主要工作内容

|  |  |  |
| --- | --- | --- |
| **服务项目** | **数量/单位** | **服务内容及要求** |
| 机房环境监测运维服务 | 1项 | 机房环境监测与运维（设备包含但不限于：消防系统、动环监控系统、UPS不间断电源、门禁系统、精密空调等） 1.UPS（不间断电源）维护（艾默生4组电池柜60KVA）：定期进行UPS主机及电池组检测，如UPS与市电线路之间的切换试验。对未接入UPS的关键设备进行线路的调整；检查记录UPS运行参数，为用户提供整改完善意见和建议。 2.机房精密空调与配电设备维护（2台艾默生、2台海瑞弗精密空调以及新风系统）：定期检查空调设备、新风设备、主配电箱。调整精密空调设备的运行参数，保证机房始终处于适宜温湿度环境下运转；检查空调运行是否正常，换风设备运转是否正常，检查否缺少制冷剂。检查空调压缩机高、低压保护开关、干燥过滤器及其他附件。 3.消防设备维护（3组柜式七氟丙烷灭火装置）：定期检查检查火警探测器、手动报警按钮、火灾警报装置外观及试验报警功能；检查火灾警报控制器的自检、消音、复位功能及主备用电源切换功能。  4.门禁系统维护：定期对门禁系统进行检查，确保门禁电源、电压等是否正常运转。确保密码、人脸、磁卡验证功能正常可用。 5.动环监控系统维护：定期检查动环监控系统的运行情况，发生报警及时处理。 6.机房环境养护（约20组机柜）：定期对机房内部的关键信息基础设施进行除尘处理；每季度至少开展一次机房环境保洁，静电地板清洁，地面除尘、缝隙调整；检查吊顶，检查电路及照明，接地电阻测试；主接地除锈、接口紧固；防雷器检查；接地线路防氧化加固。 |
| 机房设备运维管理 | 1项 | 机房设备运维（设备包含但不限于防火墙、交换机、WAF、服务器、存储日志服务器、沙箱、全流量分析、备份一体机、态势感知、虚拟化安全、终端安全管理、集中管理等30多台。） 1.确保机房内关键基础设备处于正常运行状态，定期进行硬件状态检查、系统状态检查、线缆连接情况检查，维修故障部件。 2.协助我中心开展应急故障处理、系统运维管理、系统升级、病毒查杀、网络配置等工作。 3.定期做好各种重要数据和系统的备份，当数据受损坏时，应提供数据恢复方案,并尽力提供无偿恢复服务。  4.对机房内所有设备每季度至少开展一次全面的保洁工作。 |
| 网络设备运维服务 | 1项 | 中心内部网络维护（设备包含但不限于核心交换机、约60台楼层交换机、约50台无线AP等网络设备）： 1.定期对中心内部网络进行测试，按需对交换机等网络中继设备进行配置调整、性能调优等，保障网络顺畅、稳定。 2.对网络核心设备做日常维护，检查设备运行状态、物理状态， 3.定期检查设备的系统日志文件，系统错误记录，分析系统存在的问题并解决问题。 4.重大故障调度配合、及时到场协助抢修； 5.机房网络设备及线路巡检服务：提供现场巡检服务，并按时提供巡检报告。 |
| 信息安全运维服务 | 1项 | 提供软件维护（虚拟化平台、在机房的各类系统服务器、存储服务器、防火墙、上网为管理器等）。 1.绘制与当前运行情况相符的网络拓扑结构图；划分不同的子网或网段，为各子网、网段分配地址段。 2.定期对网络设备运行状况、网络流量、用户行为等进行检查记录，发现问题后要及时与我方对接处理。 3.定期检查网络边界处的攻击行为，如端口扫描、强力攻击、木马后门攻击、拒绝服务攻击、缓冲区溢出攻击、IP碎片攻击和网络蠕虫攻击等。 4.检查各类安全防护的配置策略：定期检查安全登录网络设备的用户情况和各操作系统和数据库系统的用户情况，以及用户口令使用情况，定期检查各主机是否启用远程管理的功能和是否采用了相应的安全措施，定期检查是否启用访问控制功能。 5.定期进行系统升级和病毒查杀。 6.定期检查并发现操作系统、数据库、中间件等的漏洞，并及时打补丁。 |
| 办公电脑运维服务 | 1项 | 现场对PC、笔记本等办公电脑设备（约600台）的日常运维和故障处理等。 1.故障检查与维修：包含计算机硬件拆卸组装；各类外设安装和维护；系统软件、操作系统安装、应用软件安装及维护。 2.日常运维：所有办公电脑进行除尘、保洁；电脑系统各类软件升级；驱动程序安装；病毒查杀和防范；重要数据的备份。  3.电脑网络故障诊断排除及维护管理，网络设备安装、设置、调试及检测。 4.建立电子信息设备技术档案。 |
| 打印机、复印机、扫描仪等办公电子设备运维服务 | 1项 | 负责我中心的所有打印机、复印机、扫描仪等办公电子设备（约200台）的的日常运维和故障处理等。 1.及时对打印、复印设备进行检修，及时准确的处理日常工作中打印、复印等相关设施设备出现的问题，排除故障；  2.为正在使用的打印机、复印机和耗材提供的零件进行更换（耗材由我中心提供），安装驱动，设置共享等。 3.不定期对中心职工进行设备使用的培训，以减少人为设备故障的产生。 4.严格遵守打印机、复印机耗材添加规范，使耗材添加不会影响到主耗材的寿命和使用效果。  5每年对中心所有登记在册的电子信息类设备进行除尘、保洁全覆盖。 |
| 安全培训服务 | 1项 | 按照信息安全等级保护制度及中心相关管理工作需要，邀请区内外网络信息安全管理方面的专家进行中心内部的信息安全管理知识培训，每年至少组织1次。 |

五、维保工作要求：

1.驻场服务。提供至少2名技术工程师驻场服务（按我中心时间上下班），人员要求大专以上信息技术相关学历，35岁以下，至少3年或以上IT相关从业经验，具备包括终端主机、网络、机房设备维护的工作经历、技能以及相关专业资质，熟悉Windows、Linux等操作系统及电脑外设、打印机等软硬件日常安装、维护故障处理，熟悉网络设备安装调试。驻场工程师保持相对固定，不得随意更换，全年（包括所有的节假日期间）提供不少于2名工程师在常驻本地，确保满足响应时间要求，协助用户制订日常运行管理规范和设备运行应急预案；当现场工程师及其他支持方式无法解决问题或技术力量不足时，服务方应及时提供后援技术支持和补充。服务期间必须遵守中心制定的各项关于机房设备及业务系统运维的管理制度，并需要签订保密协议。服务方技术团队技术人员需具备以下资质：网络认证证书、网络安全工程师认证证书、信息安全认证工程师。（工作地点为南宁市金洲路18号、桃源路82号）

2.定期巡检。按照工作计划要求，定期对系统进行预防性维护，包括检查系统状态、设备清洁、系统备份，以及与客户工程师的技术交流，并提供巡检报告。

3.服务响应及技术支持。一般性故障由驻场工程师负责处理，30分钟内到现场处置（含节假日期间），重大活动时驻场工程师全天现场待命；如遇驻场工程师无法处理重大故障，维保公司技术团队应在2小时内到达现场，协助我中心完成故障定位和处置工作，必要时协调相关厂商技术人员进行免费技术支持。

4.免费提供部分备品备件及相关耗材。在本地储备相应设备维保的备品备件及相关耗材（如网线、水晶头、电源线、数据线、电池等），确保在出现故障时，及时更换。

5.提交服务报告。根据信息管理部门要求提供服务报告，内容如下：

|  |  |  |
| --- | --- | --- |
| **服务** | **报告内容** | **提交时间** |
| 日常运维服务报告 | 运维月/季/年报告 | 月度/季度/年度 |
| 重大事件服务报告 | 重大事件服务报告 | 按事件发生情况 |
| 巡检报告 | 巡检工作记录 | 月度/季度 |
| 设备维修 | 设备维修单 | 5X8驻场/其余时间电话 |
| 系统/网络优化分析 | 系统/网络优化建议 | 按用户计划 |

广西壮族自治区疾病预防控制中心

2022年6月13日